KIM-Client

Installations- und Betriebshandbuch

Version 2.01
vom 29.01.2024

Öffentlich

Connecting
your world.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Ziel und Zweck

Das vorliegende Dokument stellt Informationen zur Installation und Betrieb des KIM-Clients bereit.

1.2 Zielgruppe

Dieses Dokument richtet sich an all diejenigen, die den KIM-Client installieren müssen oder Informationen zum Betrieb des KIM-Clients benötigen.

1.3 Abgrenzung

Das vorliegende Dokument beschreibt keine Schnittstellen des KIM-Clients. Informationen zu Schnittstellen finden sich in den gematik-Spezifikationen zum KIM-Client. Zusätzliche Schnittstellen als dort beschrieben werden gesondert dokumentiert.

2 Vorbemerkung

Die Installation des KIM-Clients ist erforderlich, um KIM-E-Mail-Adressen einzurichten und zu konfigurieren, sowie den Fachdienst zu erreichen.

Dabei gliedert sich das Dokument in drei Teile:

1. *Installation,*
2. *Betrieb sowie*
3. *E-Mail-Client-Konfiguration*

Im ersten Teil finden Sie Informationen zum Bezug sowie die Installation des KIM-Clients.

Der zweite Teil beschreibt nicht nur den Aufbau der Anwendung, sondern auch die Konfiguration im Detail.

Der dritte Teil führt in die Anbindung von E-Mail-Clients ein und soll Ihnen den Integrationsprozess erleichtern.

Die Clientinstallation beschränkt sich auf definierte Betriebssystemkonfigurationen und wird im Kapitel 3.1 „Systemvoraussetzungen“ beschrieben.

Teilweise wird noch auf den Namen KOM-LE statt KIM referenziert. Diese beiden Abkürzungen sind synonym zu betrachten.

Wichtiger Hinweis:

Gelegentlich unterscheidet sich die Konfiguration einiger Parameter in Abhängigkeit von der Zielumgebung. Dieses Dokument beschreibt die Konfiguration in der RU (Realisierungsumgebung) und PU (Produktionsumgebung)

<u>RU:</u>

Verwenden Sie die Konfiguration RU für die Installationen, in denen Sie einen TU/RU-Konnektor einbinden wollen. Diese Umgebung ist für Hersteller und Anbieter von SW-Komponenten sowie als Testumgebung für Dienstleister (auch DVO) gedacht und verwendet Testkarten und keine Echtdaten.

<u>PU:</u>

Nutzen Sie die Konfiguration PU ausschließlich für die Installation in einer Wirkumgebung (Echtdatenumgebung) in einer medizinischen Einrichtung.

Der KIM-Client ermöglicht auch die Einrichtung einer KIM-E-Mail-Adresse. Eine Anleitung hierzu finden Sie in Kapitel 4.3.1.

Die verwendeten Grafiken besitzen ggf. andere Versionsbezeichnungen. Dies ist jedoch nicht relevant, solange die inhaltliche Darstellung der Grafiken übereinstimmt.

3 Client-Installation

3.1 Systemvoraussetzungen

Der KIM-Client kann auf zahlreichen Betriebssystemen installiert werden. Dabei hängen die einwandfreie Installation und der Betrieb von der Konfiguration der Umgebung ab.

Eine Konfiguration setzt sich zusammen aus

- *Betriebssystemtyp (z.B. Windows 11)*
- *Hardware-Architektur einschl. Busbreite (z.B. Windows x86, LINUX x64)*
- *Ausprägung des Betriebssystems, z.B. Windows 11 Pro (Professional), ggf. notwendiges Service Pack*

Folgende Tabelle stellt die unterstützten Betriebssystemkonfigurationen dar:

Betriebssystem	Busbreite	Ausprägung
Windows 10	64-bit	Pro
Windows 11	64-bit	Pro
Windows Server 2016	64-bit	Standard

Tabelle 1: Übersicht unterstützter Betriebssystemkonfigurationen

Die technischen Servervoraussetzungen hängen stark von der zu erwartenden Last bzgl. Anzahl und Größe der zu verarbeitenden Mails ab.

Als Minimalkonfiguration wird empfohlen:

- Arbeitsspeicher ≥ 16 GB
- Prozessorcores ≥ 8 Cores
- Festplatte 1 TB

Für eine performante Nutzung von KIM 1.5+ sollten folgende Voraussetzungen ergänzend erfüllt sein:

- Arbeitsspeicher ≥ 16 GB
- Festplatte 2 TB
- Internet-Anbindung ≥ 25 Mbit/s

Hinweis:

Bitte beachten Sie, dass die Performance auch von weiteren Parametern, wie z.B. der Netzwerkkonfiguration und dem sonstigen Lastverhalten Ihrer Infrastruktur abhängen.

3.2 Einführung und weitere Voraussetzungen

3.2.1 Einführung

KIM baut auf bereits vorhandene Komponenten der Telematik-Infrastruktur auf. Stellen Sie daher sicher, dass Sie die in den nachfolgenden Kapiteln beschriebenen technischen Voraussetzungen einhalten und Informationen zur Verfügung haben.

3.2.2 Weitere Voraussetzungen

Um den KIM-Client installieren und sich für KIM registrieren zu können, müssen Sie folgende Hardware bereithalten:

- *SMC-B und ggf. HBA*
- *Konnektor*
- *Kartenlesegerät*

Diese Komponenten müssen für den Zugang zur Telematikinfrastruktur bereits eingerichtet sein, und der Zugang zur Telematikinfrastruktur muss möglich sein. Eine Offline-Konfiguration der Komponenten reicht nicht aus!

Insbesondere sollten Sie folgende Informationen zur Hand haben:

- *Konnektor-Rechnername oder IP-Adresse*
- *Anmeldedaten für Managementoberfläche des Konnektors*
- *Aufrufkontext, unter dem der KIM-Client die zu verwendenden Karten finden kann*
- *Ihre Anmeldedaten (z.B. PINs)*
- *RegID zur Registrierung einer E-Mail-Adresse*

Hinweise:

Der Aufrufkontext wird vom KIM-Client zur Suche von verfügbaren Karten verwendet. Stellen Sie sicher, dass alle zu verwendenden Karten diesem Aufrufkontext zugewiesen sind. Sie können den Aufrufkontext an der Management-Oberfläche Ihres Konnektors ermitteln.

Stellen Sie ebenfalls sicher, dass Sie über Administrationsrechte auf den Installationsrechnern verfügen.

Bei eingeschalteter TLS-Pflicht am Konnektor muss der ungesicherte Zugang zum Dienste-verzeichnisdienst (DVD) möglich sein. Aktivieren Sie ihn folgendermaßen[1]:

- *Melden Sie sich an der Managementkonsole des Konnektors an.*
- *Aktivieren Sie am Konnektor über Netzwerk→Allgemein→Clientsystemeinstellungen→Ungesicherter Zugriff auf Diensteverzeichnisdienst.*

Bei ausgeschalteter TLS-Pflicht am Konnektor muss am Konnektor „Keine Authentifizierung“ ausgewählt sein.

[1] Die Beschreibung bezieht sich auf den secunet-Konnektor. Die Aktivierung erfolgt bei anderen Konnektoren ggf. abweichend.

3.3 Windows Betriebssysteme

3.3.1 Einführung

Die Installation für Windows-Betriebssysteme erfolgt mittels Installationspaket.

Während der Installation wird ein Deinstallationsskript bereitgestellt.

Die Installation ist für alle Windows-Betriebssysteme ähnlich. Daher wird der Vorgang in diesem Kapitel für alle Windows-Betriebssysteme zusammengefasst. Soweit sich Abweichungen vom Regelinstallationsprozess ergeben, werden diese explizit beschrieben.

Die Installation ist selbsterklärend. Für alle Betriebssysteme steht jeweils eine GUI-basierte Installation zur Verfügung.

Dieses Kapitel wird Sie Schritt für Schritt durch die Installation des KIM-Clients auf Windows-Betriebssystemen führen.

3.3.2 KIM-Client-Download vom Webportal

Um KIM installieren und sich für KIM registrieren zu können, müssen Sie sich zuerst am KIM-Webportal anmelden. Die Anmeldeadressen lauten:

- *Aus dem Internet:*
  - *Referenzumgebung (RU)*
    https://webportal-ref.eqxffm.gem-vpn-zugd-tsi.de/
  - *Produktionsumgebung (PU)*
    https://webportal.eqxffm.gem-vpn-zugd-tsi.de/

Aus der TI:

- *Referenzumgebung (RU)*
  https://webportal-ref.eqxffm.tsi.kim.telematik-test

- *Produktionsumgebung (PU)*
  https://webportal.eqxffm.tsi.kim.telematik

Erläuterung:

„Aus der TI“ bedeutet den Zugriff auf das KIM-Webportal über den Konnektor. Dieser Zugriff erfolgt nicht über das Internet. Wenn Sie die Einträge in der hosts-Datei richtig konfiguriert und die Routen richtig eingetragen haben, sollten Sie auch das Webportal über die Telematik-Infrastruktur erreichen können. Sofern das Webportal über die TI nicht erreichbar ist, überprüfen Sie bitte noch einmal die Konfiguration der hosts-Datei (siehe Kapitel 3.4.2) sowie die Routen gem. Kapitel 3.4.3.

Hinweis:
Das Webportal stellt sich für alle Umgebungen ähnlich dar. Daher wird nachfolgend der Zugriff auf das Webportal am Beispiel Referenzumgebung (RU) gezeigt.

Geben Sie diese Adresse in Ihren Web-Browser ein:

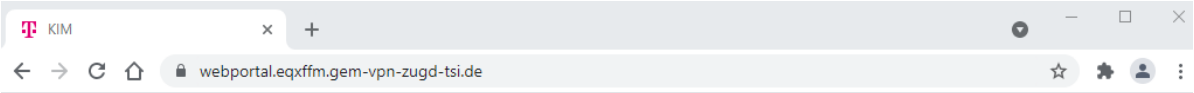

Abbildung 1: Windows – Aufruf des Webportals

Es wird die Login-Seite des KIM-Webportals angezeigt:

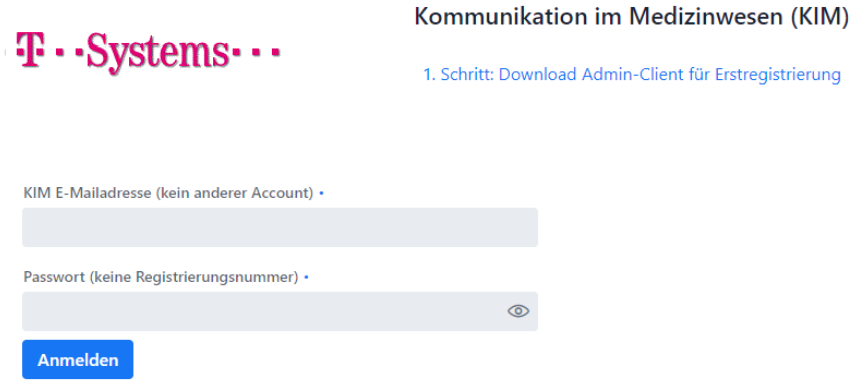

Abbildung 2: Windows – Login-Seite des KIM-Portals

Folgen Sie dem Link „1. Schritt: Download KIM-Client für Erstregistrierung“:

Abbildung 3: Windows – Erstregistrierungslink im KIM-Portal

Geben Sie in folgender Maske Ihre Registrierungsnummer und das Initialkennwort[2] an:

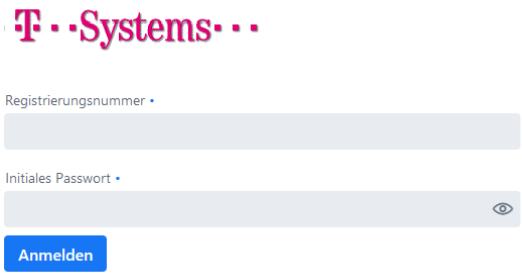

Abbildung 4: Windows – KIM-Portal – Anmeldung für Software-Download

Sie gelangen in den Download-Bereich:

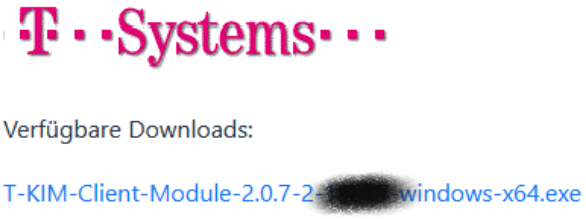

Abbildung 5: Windows – KIM-Portal – Download-Bereich

Laden Sie sich den aktuellen KIM-Client herunter.

Sie können, je nach Web-Browser zunächst den KIM-Client lokal speichern, und später aus dem Dateiexplorer starten, oder direkt ausführen lassen.

Hinweis:
Wir empfehlen Ihnen, den KIM-Client zunächst lokal zu speichern, so dass Sie im Falle eines Abbruchs der Installation diesen nicht erneut herunterladen müssen.

[2] Das Initialkennwort lautet 00000, also fünfmal die Null.

3.3.3 Installation

Um den KIM-Client zu installieren, führen Sie bitte das Installationspaket zum KIM-Clientmodul aus. Bitte beachten Sie die Installationsvoraussetzungen, die in den Kapiteln 3.1 und 3.2.2 beschrieben sind.

Das Installationspaket sollten Sie entsprechend Kapitel 3.3.2 heruntergeladen haben.

Das Installationspaket beinhaltet einen Assistenten, der Sie durch die gesamte Installation des KIM-Clientmoduls führt.

Der erste Dialog ist der Willkommensdialog. Sie erhalten dort noch einmal eine Versionsinformation zum Clientmodul. Des Weiteren wird automatisch überprüft, ob bereits eine Version des KIM-Clients installiert wurde.

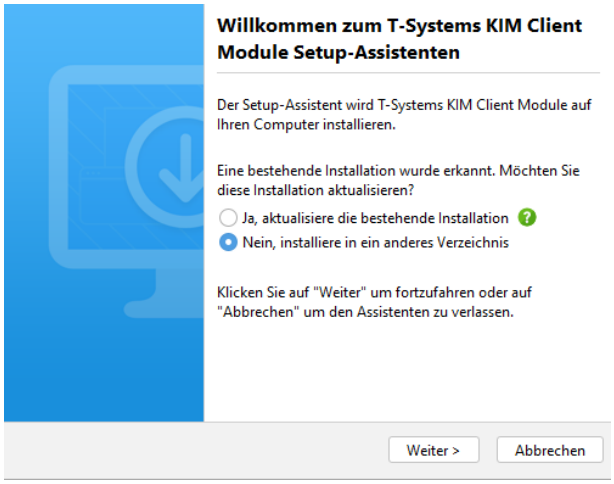

Abbildung 6: Windows – KIM-Clientmodul-Installationspaket – Willkommensdialog

Für eine Aktualisierung der bestehenden Installation wählen Sie „Ja, aktualisiere die bestehende Installation“.

Wichtiger Hinweis:
Aus Sicherheitsgründen ist auch für eine bestehende Installation im Fall einer Aktualisierung die erneute Eingabe von Zugangsdaten (z.B. zum Konnektor, für die Basisauthentifizierung) erforderlich.

Für eine neue Installation wählen Sie „Nein, installiere in ein anderes Verzeichnis“ aus.

Nach Ihrer Wahl drücken Sie den „Weiter“-Button, um in den nächsten Dialog zu gelangen.

Um mit der Installation fortfahren zu können, müssen Sie den Lizenzbestimmungen zustimmen:

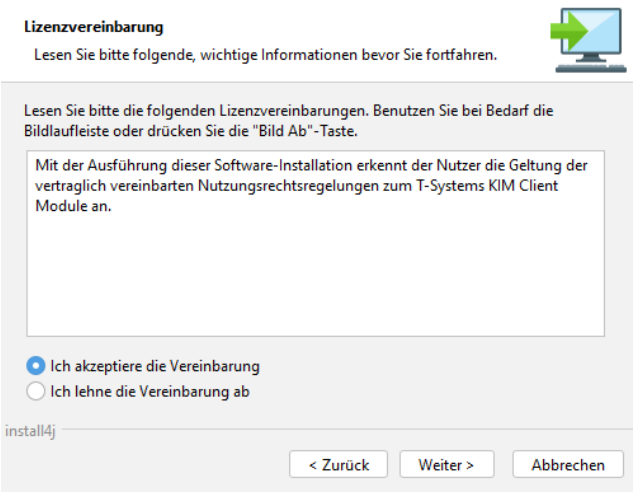

Abbildung 7: Windows – KIM-Client-Installationspaket – Lizenzbestimmungen

Legen Sie zunächst fest, in welchem Ordner der KIM-Client installiert werden soll:

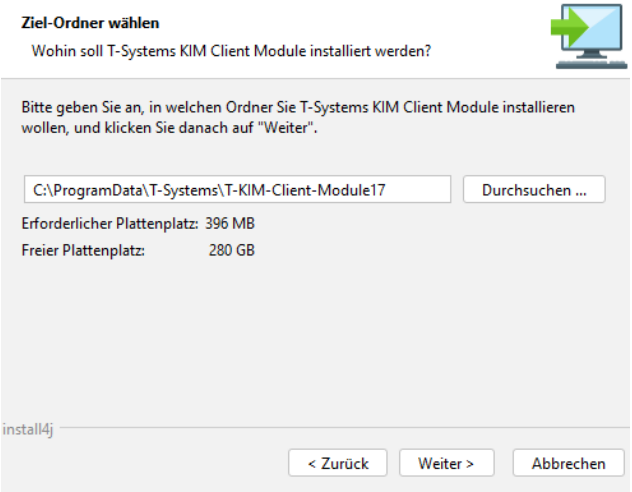

Abbildung 8: Windows – KIM-Client-Installationsverzeichnis

Geben Sie dann die TI-Umgebung an, für die Sie installieren wollen. Passen Sie bei Bedarf die Vorauswahl an.

Wichtiger Hinweis:

Für eine **Wirkbetriebsinstallation** wählen Sie **PU** aus. PU ist bereits vorausgewählt.

Handelt es sich dagegen um eine **Testinstallation**, für die keine Echtdaten verwendet werden (z.B. für DVO, SW-Hersteller usw.) wählen Sie bitte **RU** aus.

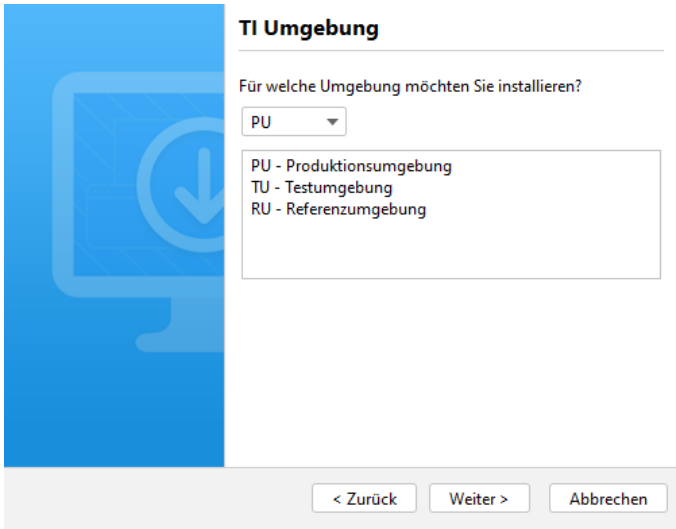

Abbildung 9: Windows – KIM-Client-Installationspaket – TI-Umgebung

Konfigurieren Sie im nächsten Schritt Ihre Einsatzumgebung:

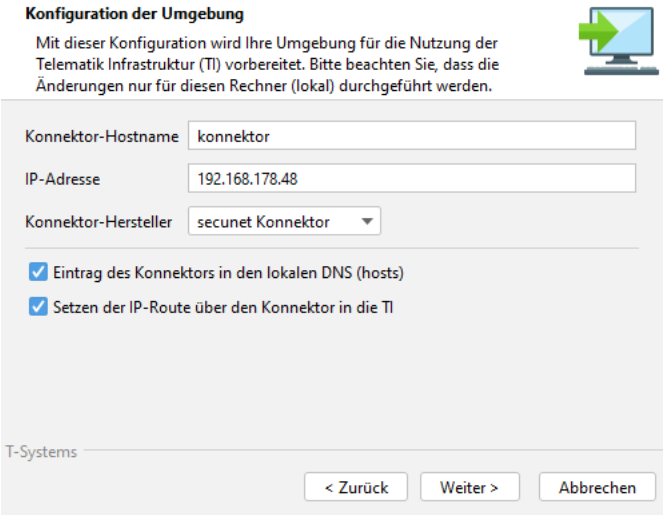

Abbildung 10: Windows – KIM-Client-Installationspaket – Lokale Umgebung

Geben Sie bei Konnektor-Hostname die Bezeichnung des Hosts ein, die für den Konnektor verwendet werden soll. Im Standardfall ist die, wie vorgegeben „konnektor“.

Tragen Sie bei „IP-Adresse“ die Adresse des Konnektors in Ihrer lokalen Umgebung ein. Wählen Sie den Konnektorhersteller aus.

Sofern Sie einen DNS-Hosteintrag benötigen, setzen Sie den Haken bei „Eintrag des Konnektors in den lokalen DNS (hosts)“.

Sie können das Routing über den Konnektor einrichten. Haken Sie dazu „Setzen der IP-Route über den Konnektor in die TI“ an.
Diese Einstellung passt die lokale Routing-Tabelle so an, dass die erforderliche permanente Route zum Konnektor lokal konfiguriert wird. Eine manuelle Konfiguration ist dann nicht mehr erforderlich.

Sofern das Routing für den KIM-Client in Ihrer Netzwerkumgebung nicht über den Konnektor erfolgen soll, setzen Sie keinen Haken.

Wichtiger Hinweis zum Routing:

Das automatische Setzen der Route funktioniert nur dann ohne manuelle Konfiguration, wenn sich KIM-Client und Konnektor im selben Netzsegment befinden (dies ist der Regelfall in kleineren Einrichtungen).

Ist dies nicht der Fall, sollten Sie die IP-Route von Hand setzen und dies nicht das Installationspaket machen lassen. Lassen Sie sich ggf. von Ihrem DVO, Ihrem IT-Support bzw. Ihrer IT-Fachabteilung beraten.

Es gibt mehrere Lösungswege, um auch Segment-übergreifend den Konnektor erreichen zu können. Zwei davon sollen hier kurz skizziert werden:

1. Ausstattung des Rechners mit einer zweiten Netzwerkkarte.
Prüfen Sie, ob es möglich ist, eine zweite Netzwerkkarte für das andere Segment im Rechner zu verbauen. Konfigurieren Sie Ihren Rechner so, dass der Verkehr lokal in das andere Segment geroutet werden kann. Setzen Sie NAT ein.

2. Richten Sie lokal eine Route auf einen „Durchgangsrouter“ ein. Konfigurieren Sie den Router so, dass der vom KIM-Client-Rechner kommende und für den Konnektor bestimmte Verkehr vom Router an den Konnektor weitergeleitet werden kann.

Gehen Sie weiter zum Einstellen des Aufrufkontextes.

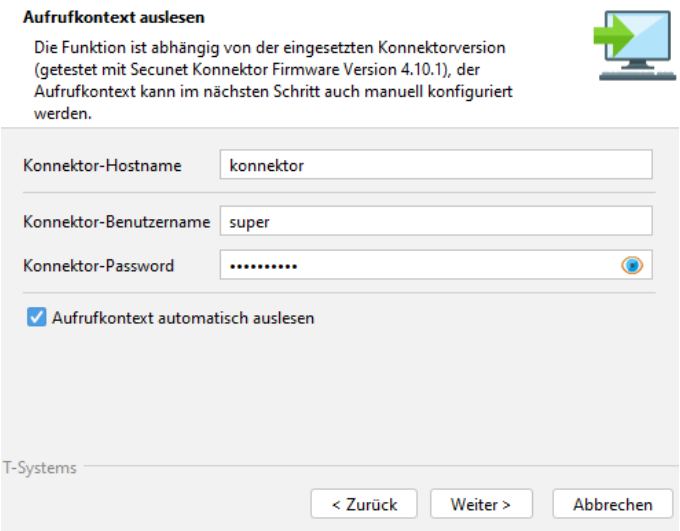

Abbildung 11: Windows – KIM-Client-Installationspaket – Aufrufkontext auslesen

Um automatisiert die Aufrufkontexte auslesen zu können, setzen Sie das Häkchen und geben die Anmeldedaten für Ihren Konnektor ein (Ggf. verwenden Sie einen von Abbildung 11 abweichenden Benutzernamen).
Wenn Ihr Konnektor das Auslesen der Aufrufkontexte unterstützt, können Sie in der folgenden Maske den zu verwendenden Kontext auswählen:

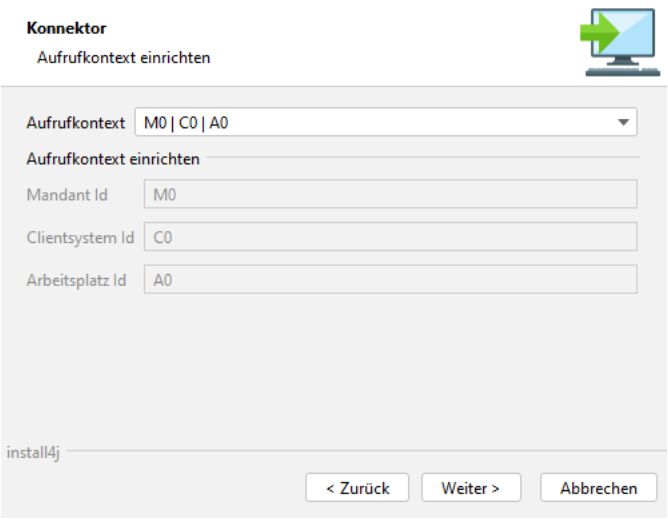

Abbildung 12: Windows – KIM-Client-Installationspaket – Aufrufkontext halbautomatisch einrichten

Sofern Sie den Kontext nicht auslesen wollen, oder dies von Ihrem Konnektor nicht unterstützt wird, können Sie im nachfolgenden Dialog den Aufrufkontext direkt konfigurieren. Achten Sie darauf, dass der Mandantenkontext gültig ist. Der Mandantenkontext darf dabei folgende Zeichen enthalten:

- Ziffern 0 .. 9
- Buchstaben a .. z und A .. Z

Alle sonstigen Zeichen sind nicht erlaubt, auch wenn Ihr Konnektor diese unterstützt.

Drücken Sie nach einer individuellen Konfiguration auf „Weiter“.

Um die TLS-Verbindung zwischen KIM-Clientmodul und Konnektor bereits während der Installation zu aktivieren, markieren Sie das nachfolgende Feld „Soll die Verbindung verschlüsselt werden?“. Sofern Sie keine Verschlüsselung konfigurieren wollen, nehmen Sie ein etwaiges Häkchen heraus und drücken dann auf Weiter. Sie kommen dann zu „Konfiguration E-Mail-Client/Clientmodul“. Siehe hierzu weiter unten.

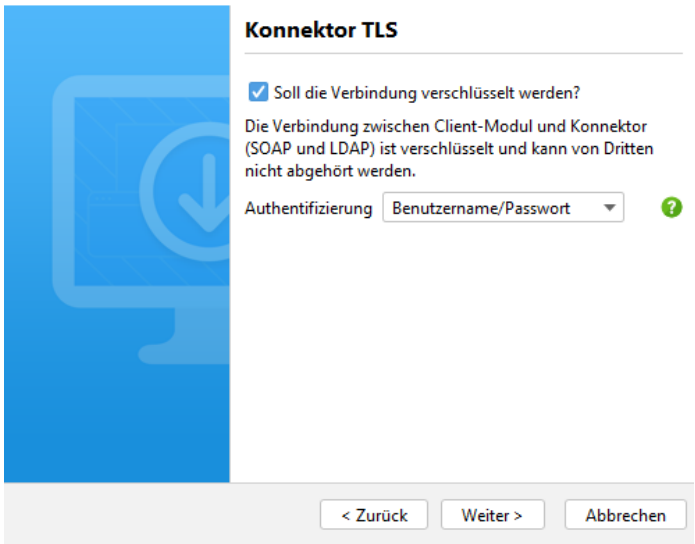

Abbildung 13: Windows – KIM-Client-Installationspaket – Konnektor-TLS

TLS-Konfiguration

Überspringen Sie diesen Abschnitt, wenn Sie keine Verschlüsselung ausgewählt haben und setzen Sie die Konfiguration, wie unter „Konfiguration E-Mail-Client/Clientmodul“ beschrieben, fort.

Sofern Sie eine Verschlüsselung ausgewählt haben (Haken gesetzt), können Sie hier folgende Einstellungen vornehmen:

- Keine Authentifizierung
  Stellen Sie hier sicher, dass auch am Konnektor die Authentifizierung ausgeschaltet ist.
- Benutzername/Passwort
  Es muss am Konnektor der entsprechende Benutzername konfiguriert sein.
- Zertifikat

Sofern Sie keine Authentifizierung ausgewählt haben, kommen Sie mit „Weiter“ zu „Konfiguration E-Mail-Client/Clientmodul“. Siehe hierzu weiter unten!

Bei der Auswahl von Benutzername/Passwort werden Sie im nachfolgenden Dialog gebeten, die entsprechenden Angaben zur Authentifizierung zu vervollständigen:

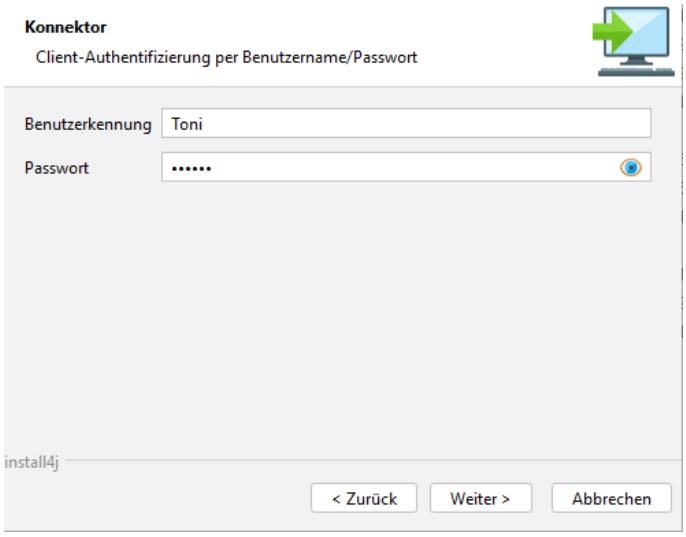

Abbildung 14: Windows – KIM-Client-Installationspaket – Clientauthentifizierung per Benutzername und Passwort

Tragen Sie hier ihre individuelle Benutzerkennung ein („Toni“ ist nur ein Beispiel!).

Wenn Sie eine zertifikatsbasierte TLS-Verbindung gewählt haben, können Sie im folgenden Dialog Anpassungen vornehmen:

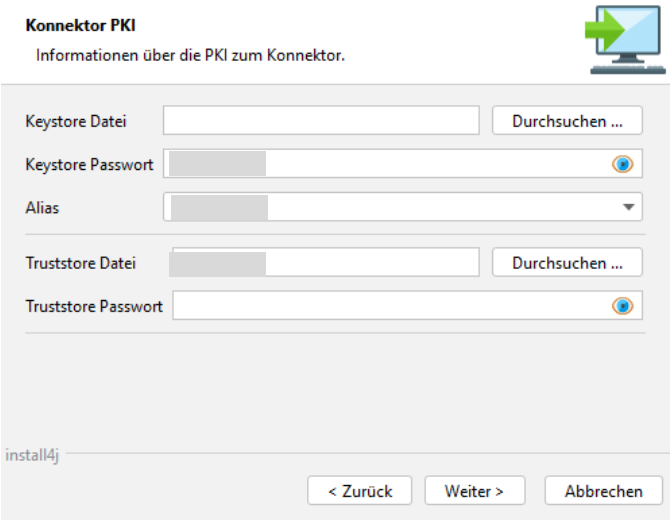

Abbildung 15: Windows – KIM-Client- Installationspaket – Client-/Serverauthentifizierung per Zertifikat

Geben Sie unter „Keystore Datei“ die Zertifikatsdatei an, die Sie für die Clientauthentifizierung verwenden wollen. Ergänzen Sie das „Keystore Passwort“. Der eingetragene „Alias“ entspricht dem Rechnernamen, auf dem der KIM-Client installiert wird.

Geben Sie ggf. auch einen Truststore (optional) an. Dieser ermöglicht es dem KIM-Client, nur vorher bestimmte Zertifikate einer Gegenseite zu akzeptieren. Hinterlegen Sie hier dann auch das Truststore Passwort.

Hinweis:
Zur Konfiguration der TLS-Kommunikation lesen Sie bitte auch die ergänzenden Hinweise in Kapitel 4.6.11.

Drücken Sie „Weiter“, um in den folgenden Dialog zu kommen. Dort können Sie die Kommunikationsparameter zwischen E-Mail-Client und KIM-Clientmodul festlegen:

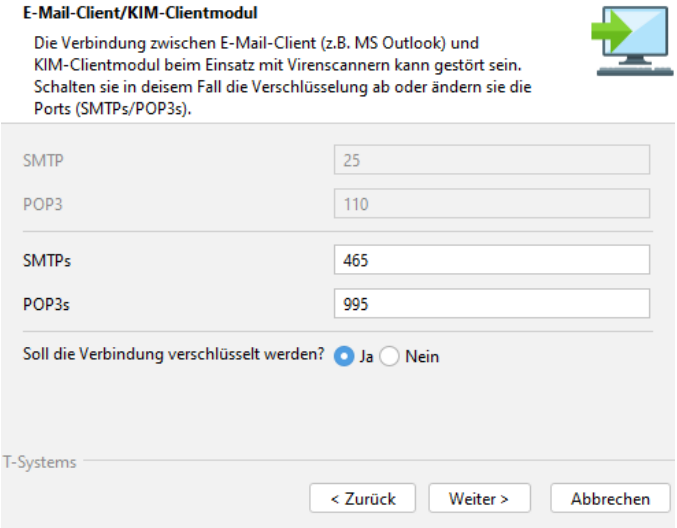

Abbildung 16: Windows – KIM-Client-Installationspaket – E-Mail-Client/Clientmodul

Wählen Sie zum einen aus, ob die Verbindung verschlüsselt werden soll, zum anderen, welche Ports der KIM-Client zur Kommunikation vom E-Mail-Client aus verwenden soll.

Konfigurieren Sie die Ports und die Verschlüsselung entsprechend Ihren Erfordernissen. Drücken Sie dann auf „Weiter“.

Im nächsten Schritt können Sie den Mailcache konfigurieren.

Hinweis:
Der Mailcache ist optional und Bestandteil des KIM-Security-Interfaces. Er stellt weitere Anforderungen an die Einsatzumgebung. Weitere Informationen zum Mailcache erhalten Sie in Kapitel 4.4.3 ff.

Für eine Installation ohne Mailcache (Standardinstallation) bleibt die Checkbox bei „Soll der Mailcache benutzt werden?“ leer.

Sofern Sie einen Mailcache einrichten wollen, markieren Sie die Checkbox „Soll der Mailcache benutzt werden?“:

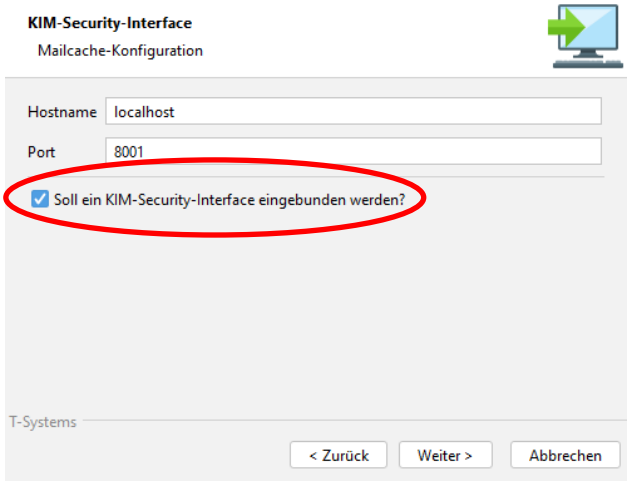

Abbildung 17: Windows – KIM-Client-Installationspaket – Einbindung des Mailcaches

Drücken Sie danach auf „Weiter“.

Die letzte Konfiguration ermöglicht es Ihnen, einen lokalverfügbaren Virenscanner über die Betriebssystemschnittstelle (AMSI) einzubinden:

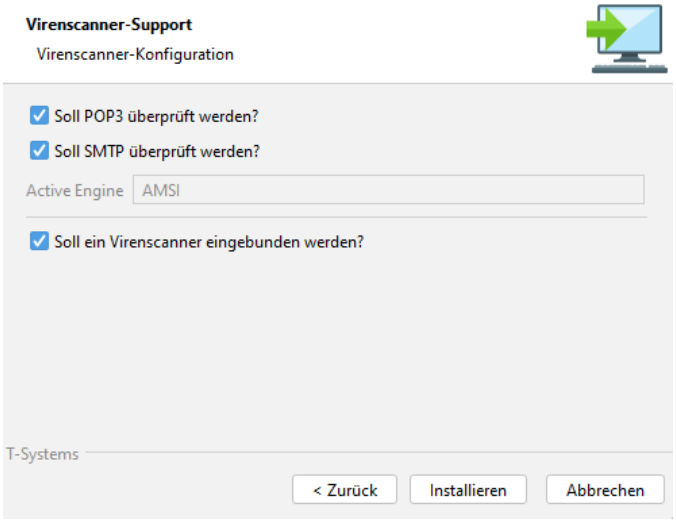

Abbildung 18: Windows – KIM-Client-Installationspaket – Virenscanner-Support

Sofern Sie Ihren lokalen Virenscanner einbinden wollen, setzen Sie das Häkchen bei „Soll der Virenscanner benutzt werden?“. Dabei nutzt der KIM-Client ihren über das Betriebssystem verfügbaren Virenscanner.

Falls Sie Ihren lokalen Virenscanner nicht einbinden wollen (Standardinstallation), entfernen Sie das Häkchen.

Weitere Informationen zum Einbinden eines lokalen Virenscanners finden Sie in Kapitel 4.4.4.

Nach Drücken des Buttons „Installieren“ wird der KIM-Client auf Ihrem System installiert.

Legen Sie im letzten Schritt nach der Installation fest, ob ein Desktop-Link erstellt bzw. der KIM-Client als Dienst/Daemon bereitgestellt werden soll.

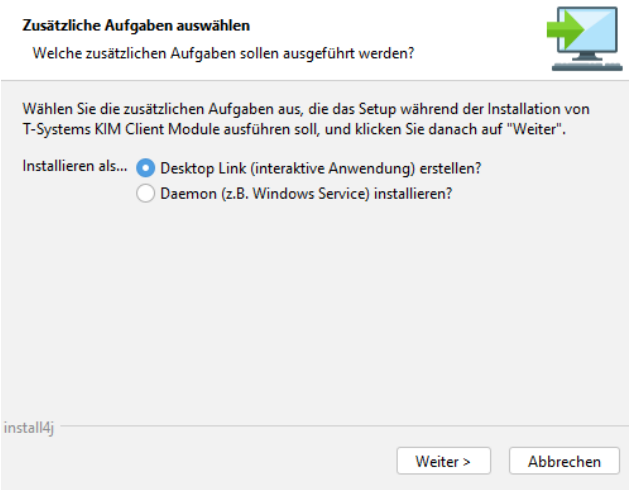

Abbildung 19: Windows – KIM-Client-Installationspaket – Zusätzliche Aufgaben

Hinweis:

Diese Entscheidung ist individuell vorzunehmen und hat keinen Einfluss auf die Kernfunktionalität des KIM-Clients.

Sie sollten einen Desktop-Link einrichten, wenn

- es sich um ein Einzelplatz-System handelt und Statusmeldungen des KIM-Client dargestellt werden sollen und der Zugriff nur lokal auf dem PC erfolgen soll.

Verwenden Sie „Daemon“ wenn es sich um eine Installation

- auf einem (Praxis-) Server handelt (zentraler Zugriff), oder wenn

- auf einem (Praxis-) Client die Ausgabe von Statusmeldungen unterdrückt werden soll.

Legen Sie abschließend das Startverhalten des KIM-Clients fest.

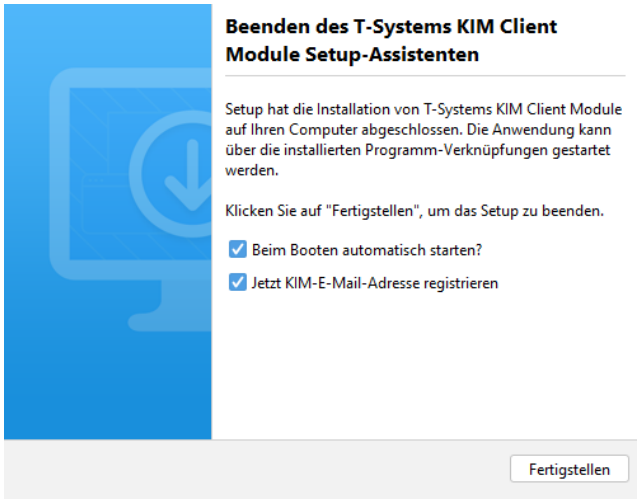

Abbildung 20: Windows – KIM-Client-Installationspaket - Startverhalten

Sie können im Anschluss an die erfolgreiche Installation sofort Ihre KIM-E-Mail-Adresse registrieren. Sofern Sie hier den Haken setzen, wird der T-Wizard gestartet (siehe hierzu Kapitel 4.3.1 auf Seite 35).

Falls Sie bereits über eine KIM-E-Mail-Adresse verfügen müssen Sie keine weitere registrieren. Entfernen Sie dann das Häkchen bei „Jetzt KIM-E-Mail-Adresse registrieren“.

Mit Drücken auf „Fertigstellen“ ist die Installation abgeschlossen.

Nach einer Neuinstallation und sofern keine neue E-Mail-Adresse registriert werden soll, wird im Anschluss der Zertifikatsdownload für die weitere Konfiguration gestartet. Sofern Sie eine Neuinstallation durchgeführt haben, ist die Ausführung des Zertifikatsdownloads zwingend erforderlich. Siehe hierzu auch Kapitel 4.3.2.

3.3.4 Deinstallation

Zur Deinstallation des KIM-Clients gehen Sie bitte folgendermaßen vor:

- Öffnen Sie das Startmenü. Wählen Sie dort Einstellungen aus. Windows öffnet das Dialogfenster „Windows-Einstellungen“.
- Wählen Sie den Eintrag „Apps“ aus.

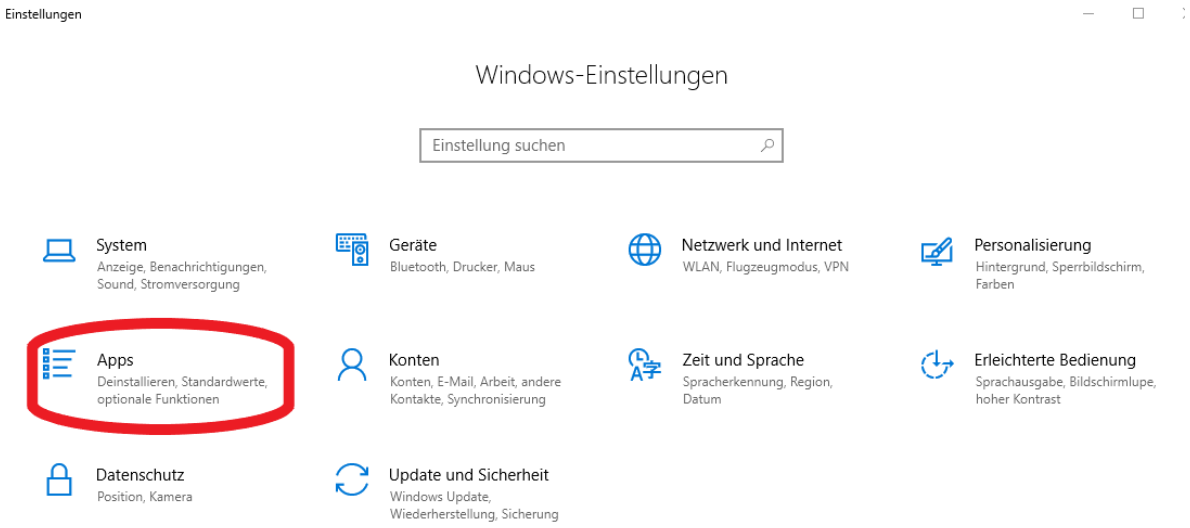

Abbildung 21: Dialogfenster „Windows-Einstellungen“

Wählen Sie auf der nachfolgenden Ansicht den Eintrag „Apps & Features“ aus. Dort erhalten Sie eine Übersicht der von Ihnen installierten Anwendungen.

Sobald Sie den Eintrag markieren, werden Ihnen zwei Schaltflächen (Ändern, Deinstallieren) angeboten.

Drücken Sie die Schaltfläche „Deinstallieren“. Es öffnet sich der Deinstallationsassistent.

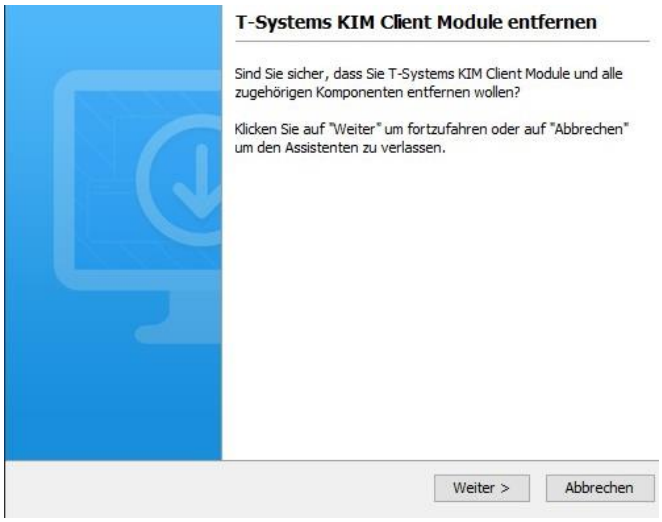

Abbildung 22: Windows – KIM-Client-Deinstallation

Drücken Sie zur Deinstallation den „Weiter“-Button. Die Deinstallation wird darauf hin automatisch gestartet. Über den Abschluss werden Sie in einem weiteren Dialog informiert. Bestätigen Sie diesen durch Drücken des „Fertigstellen“-Buttons.

Abbildung 23: Windows – Abschluss Deinstallation KIM-Client

3.4 Manuelle Konfiguration zur Installation

3.4.1 Vorbemerkung

Die in den nachfolgenden Kapiteln beschriebenen Anpassungen werden idealerweise durch das Installationsskript ausgeführt. Eine manuelle Konfiguration ist im Regelfall nicht erforderlich.

Nutzen Sie diese Beschreibungen nur dann, wenn eine automatische Konfiguration durch das Installationsskript nicht möglich ist oder korrigiert werden muss!

3.4.2 Anpassen der hosts-Datei

Hinweise:

Das Anpassen der hosts-Datei erfolgt in der Regel automatisch durch das Installationsskript.
Bei Nutzung von „DNS-SD“ ist für KIM nur noch der Konnektor in der hosts-Datei einzutragen. Alle weiteren Eintragungen (Webportal, Fachdienst) entfallen.

Um den Fachdienst über den Konnektor erreichen zu können, müssen Einträge in der hosts-Datei vorgenommen werden. Des Weiteren ist es sinnvoll, zur einfacheren Konfiguration des KIM-Clients, den Konnektor ebenfalls in der hosts-Datei einzutragen.

Hierzu gehen Sie wie folgt vor:

1. Öffnen Sie unter Windows den Datei-Explorer.
2. Wählen Sie den Speicherort der hosts-Datei aus. Diese ist unter Windows 10 und Windows 11 in folgendem Verzeichnis abgelegt:
   Windows→System32→drivers→etc
3. Öffnen Sie mit einem Editor die Datei hosts.
4. Tragen Sie die IP-Adresse des Konnektors und den während der Installation vergebenen Host-Namen durch mindestens ein Leerzeichen getrennt ein (Sofern Sie den vorgegebenen Standardnamen beibehalten haben, lautet dieser „konnektor“). Vergeben Sie einen Kommentar, der ebenfalls durch mindestens ein Leerzeichen getrennt und durch das #-Symbol angefügt ist. Der Eintrag könnte beispielsweise danach etwa so aussehen:
   192.168.178.48 konnektor # Adresse des Konnektors
   Des Weiteren müssen ggf. auch Einträge für den Fachdienst vorgenommen werden. Diese sind umgebungsabhängig:

   RU (Realisierungsumgebung):

   10.30.1.132 mail-ref.eqxffm.tsi.kim.telematik-test

   10.30.1.135 webportal-ref.eqxffm.tsi.kim.telematik-test

   PU (Produktionsumgebung):

   100.102.1.136 webportal.tsi.kim.telematik

   100.102.1.136 webportal.eqxffm.tsi.kim.telematik

   100.102.3.136 webportal.eshffm.tsi.kim.telematik

   100.102.3.136 webportal.tsi.kim.telematik

100.102.1.169	lb-mail.tsi.kim.telematik
100.102.1.169	lb-mail.eqxffm.tsi.kim.telematik
100.102.3.169	lb-mail.eshffm.tsi.kim.telematik
100.102.3.169	lb-mail.tsi.kim.telematik

5. Speichern Sie die hosts-Datei.

Wichtiger Hinweis:

Zum Anpassen der hosts-Datei benötigen Sie Administrationsrechte!

3.4.3 Einrichten der Routen

Hinweis:

Das Einrichten der permanenten Route erfolgt in der Regel automatisch durch das Installationsskript.

Um die durch die in der hosts-Datei ermittelten IP-Adressen richtig zu routen, muss die Routing-Tabelle des Rechners, auf dem der KIM-Client installiert wurde, angepasst werden.

Tragen Sie dafür folgende Routen als permanente Routen ein:

RU (Realisierungsumgebung)

route /p add 10.30.0.0 MASK 255.255.0.0 <IP-Adresse des Konnektors>

PU (Produktionsumgebung)

route /p add 100.102.0.0 MASK 255.255.0.0 <IP-Adresse des Konnektors>

Wichtiger Hinweis zur Einrichtung statischer Routen:

Das statische Routing setzt voraus, dass sich Konnektor und KIM-Client im selben Subnetz befinden. Sollte dies nicht der Fall sein, gibt es folgende Lösungsansätze:

1. Nachrüsten einer weiteren Netzwerkkarte, die so konfiguriert wird, dass der Konnektor aus dem aktuellen Subnetz direkt erreicht werden kann (lokales NAT).

2. Routen anpassen, so dass der für den Konnektor bestimmte Verkehr an einen Router weitergeleitet wird, der auch das zweite Subnetz erreichen kann. Dort muss dann ebenfalls das Routing entsprechend konfiguriert werden.

Die Konfiguration der permanenten Route für unterschiedliche Subnetze muss manuell erfolgen.

4 Betrieb

4.1 Einführung

4.1.1 Regeln zur Bildung von Kennwörtern

Wichtiger Hinweis: Bitte beachten Sie die BSI-Vorgaben zur sicheren Verwendung von Kennwörtern (siehe Anhänge A.2 und A.3)

Kennwörter (Passwörter) müssen bestimmte Kriterien erfüllen, damit sie als zulässig akzeptiert werden.

Ein Kennwort muss folgende Anforderungen erfüllen:

- Mindestens 12 Zeichen lang
- Bestehend aus mindestens drei der folgenden vier Gruppen:
  - Kleinbuchstaben [a .. z]
  - Großbuchstaben [a .. z]
  - Ziffern [0 .. 9]
  - Sonderzeichen [$ % + # - _]

Hinweis: Umlaute sowie nicht dem deutschen Alphabet zugehörige Buchstaben (z.B. ß, ê, ñ) sind nicht zulässig. Weitere als die oben in der Gruppe genannten Sonderzeichen sind ebenfalls nicht zulässig.

Handelt es sich um einen Passwortwechsel, gilt zudem folgende Anforderung:

- Das Kennwort muss sich von den fünf vorhergehenden Kennwörtern unterscheiden.

4.1.2 Regeln zur Bildung einer E-Mail-Adresse

Die E-Mail-Adresse hat grundsätzlich folgenden Aufbau:

<local part>@<domain part>

Während der <domain part> von Ihrem KIM-Anbieter festgelegt wird, können Sie den <local part> grundsätzlich selbst festlegen – vorausgesetzt, dass die E-Mail-Adresse noch in der Telematikinfrastruktur verfügbar ist.

Für die E-Mail-Adresse gelten folgende Regeln:

- *Erlaubte Zeichen:*
  - *Buchstaben a .. z*
  - *Ziffern 0 .. 9*

    - *Sonderzeichen Minuszeichen, Punkt und Unterstrich*
- *Maximale Länge von 64 Zeichen*

Wichtiger Hinweis: Bei der Eingabe von Großbuchstaben werden diese vor der Prüfung bzw. vor der Anlage der E-Mail-Adresse in Kleinbuchstaben umgewandelt.

4.1.3 Regeln zur Bildung eines Aufrufkontextes

Da KIM-Nachrichten in UTF-8-Kodierung sendet und empfängt und der Mandanten-/Aufrufkontext Teil der Kommunikation ist, unterliegt der verwendbare Kontext ebenfalls der UTF-8-Kodierung.

Um Fehler in der Verarbeitung der Kontexte zu vermeiden, sind nur folgende Zeichen erlaubt:

- Ziffern 0 .. 9
- Großbuchstaben A .. Z
- Kleinbuchstaben a .. z

4.2 Starten und Beenden des KIM-Clients

4.2.1 Vorbemerkung und Voraussetzungen

Mit der Installation des KIM-Clients werden verschiedene Komponenten installiert.

Im Windows-Startmenü finden Sie daher mehrere Anwendungen, die sich auf diese beiden Komponenten abstützen:

- T-Systems KIM E-Mail-Registrierung
- T-Systems KIM Zertifikatsdownload
- T-Systems KIM Administration Client
- T-Systems KIM Client Module

Die Auswahl der zunächst zu startenden Anwendung hängt davon ab, wie Sie Ihre Installation durchgeführt haben.

Sofern Sie eine Neuinstallation vorgenommen haben müssen Sie zunächst sowohl E-Mail-Adresse als auch Clientzertifikat konfigurieren und installieren. Dieses können Sie assistenzgestützt (siehe Kapitel 4.3) bzw. mittels Administrationsclient (siehe Kapitel 4.3.3) durchführen.

Wenn Sie lediglich ein Update auf eine bestehende Installation durchgeführt haben und bereits früher eine E-Mail-Adresse registriert hatten, können Sie das KIM-Clientmodul direkt starten.

Gleiches gilt, wenn Sie weder eine Neuinstallation noch ein Update auf eine bestehende Installation durchgeführt haben, sondern bereits eine lauffähige Anwendung vorhanden ist. Hier können Sie ebenfalls das KIM-Clientmodul direkt starten.

Nachfolgend zunächst ein kurzer Überblick zu den einzelnen Anwendungen.

4.2.1.1 KIM-E-Mail-Registrierung

Hierunter verbirgt sich der T-Wizard, der es Ihnen ermöglicht, assistenzgestützt eine E-Mail-Adresse anzulegen/ zu registrieren. Im Zuge der Registrierung wird auch ein Clientzertifikat konfiguriert.

Weitere Informationen zur Nutzung des Registrierungsassistenten erhalten Sie in Kapitel 4.3.1.

4.2.1.2 KIM-Zertifikatsdownload

Beim Zertifikatsdownload handelt es sich um einen Assistenten, der Ihnen das Herunterladen eines auf den Installationsrechner ausgestelltes Clientzertifikat aus der TI ermöglicht. Bitte beachten Sie, dass Sie den Zertifikatsdownload nur dann nutzen können, wenn Sie bereits über eine KIM-E-Mail-Adresse verfügen. Ansonsten nutzen Sie den im Kapitel 4.2.1.1 beschriebenen Registrierungsassistenten.

Ausführliche Informationen zur Verwendung des Zertifikatsdownloads finden Sie im Kapitel 4.3.2.

4.2.1.3 T-KIM-Admin-Client

Der Administrationsclient stellt Verwaltungsfunktionen zusammengefasst in einem Anwendungsfenster bereit. Hier können Sie die wichtigsten fachlichen Konfigurationsaufgaben erledigen und einen Verbindungstest durchführen.

Eine ausführliche Beschreibung zum Administrationsclient enthält Kapitel 4.3.3.

4.2.1.4 T- KIM-Clientmodul

Das Clientmodul stellt die E-Mail-Kommunikation bereit und ermöglicht Ihnen, Ihr Postfach auf dem Fachdienstserver zu erreichen. Das Clientmodul besitzt keine Oberfläche.

Hinweis:

Bevor Sie das KIM-Clientmodul in Betrieb nehmen können, müssen Sie über mindestens eine E-Mail-Adresse und ein Clientzertifikat verfügen.

4.2.2 Starten des KIM-Clientmoduls

4.2.2.1 Manueller Start aus dem Desktop (Desktop-Variante)

Sofern Sie den KIM-Client in der Desktop-Variante installiert haben, können Sie das Clientmodul aus ihrem Desktop mittels Doppelklicks auf das Icon starten:

Abbildung 24: Desktop-Icon des KIM-Clientmoduls

Das KIM-Clientmodul besitzt keine Oberfläche. Man erkennt jedoch den Start am Informationsicon unten rechts auf dem Desktop.

Hinweis: Informationsicons werden nur dann angezeigt, wenn die Installation nicht als Dienst/Daemon, sondern als Desktop-Anwendung durchgeführt wurde.

Sollte das Clientmodul nicht ordnungsgemäß gestartet werden können, so finden Sie detailliertere Hinweise in den Logdateien des KIM-Clients.

Die Logdateien befinden sich im Unterverzeichnis „logs“ des Installationsverzeichnisses zum KIM-Client.

4.2.2.2 Manueller Start aus dem Windows-Startmenü (Desktop-Variante, Server-Variante)

Sowohl in der Desktop- aus auch in der Server-Variante können Sie den KIM-Client aus dem Windows-Startmenü heraus starten.

1. Klicken Sie zunächst auf das Windows-Startmenü-Symbol (⊞) Ihres Desktops.
2. Klicken Sie auf den Button „Alle Apps >“.
3. Scrollen Sie in der Liste aller Apps bis zum Ordner „T-KIM-Clientmodul“.
4. Wählen Sie den Eintrag „T-KIM-Clientmodul“ aus.

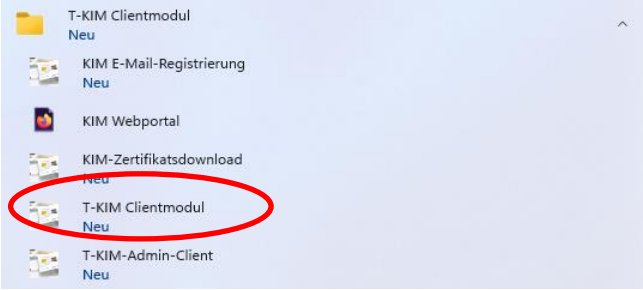

Abbildung 25: Windows-Startmenü mit geöffnetem T-Systems-Clientmodul-Ordner

4.2.2.3 Verwenden der Windows Suche

Setzen Sie den Cursor in das Windows Suchfenster und geben dann den Begriff “KIM” ein. Es werden Ihnen die entsprechend gefundenen Anwendungen zur Auswahl angeboten. Wählen Sie den Eintrag „T-KIM-Clientmodul“ aus.

4.2.2.4 Automatischer Start

Für den Fall, dass Sie bei der Installation „Beim Booten automatisch starten“ angehakt hatten, brauchen Sie sich nicht um den Start des KIM-Clients zu kümmern. Dieser wird bei jedem Boot-Vorgang automatisch ausgeführt.

Sofern es Probleme mit dem automatischen Start geben sollte, gehen Sie wie in den Kapiteln zum manuellen Start vor (siehe hierzu Kapitel 4.2.2.1 bzw. 4.2.2.2).

4.2.2.5 Manueller Start des Dienstes

Sofern Sie das Clientmodul als Dienst installiert haben, können Sie über den Taskmanager den Dienst manuell starten. Öffnen Sie dazu den Taskmanager und wählen die Liste aller Dienste aus.

Der zu startende Dienst heißt „cmdaemon“, die Beschreibung lautet „T-KIM-Clientmodul“. Wählen Sie aus dem Kontextmenü zu diesem Eintrag „Starten“ aus.

4.2.3 Beenden

4.2.3.1 Desktop-Variante

Es kann erforderlich sein, den KIM-Client von Hand zu beenden. Hierfür gehen Sie wie folgt vor:

- Wählen Sie den KIM-Client aus den Symbolen des Windows-Desktoptrays unten rechts aus. Ggf. ist es erforderlich, auch die ausgeblendeten Symbole anzuzeigen.
- Gehen Sie mit dem Mauszeiger über das Symbol des KIM-Clients.
- Drücken Sie die rechte Maustaste.
- Wählen Sie „Beenden“ aus.

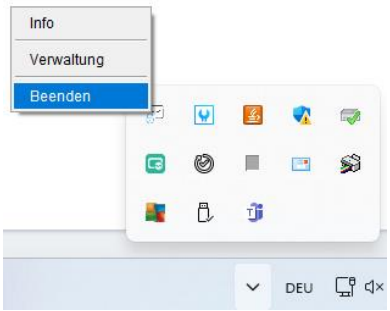

Abbildung 26: Desktop – KIM-Client – Beenden

Die Anwendung wird dann beendet. Dies kann eine kurze Zeit dauern. Sie erkennen den Abschluss des Vorgangs daran, dass das Symbol des KIM-Clientmoduls nicht mehr angezeigt wird.

4.2.3.2 Server-Variante

Sollten Sie das Clientmodul als Dienst installiert haben, können Sie über den Taskmanager den Dienst manuell beenden. Öffnen Sie dazu den Taskmanager und wählen die Liste aller Dienste aus.

Der zu startende Dienst heißt „cmdaemon“, die Beschreibung lautet „T-KIM-Clientmodul“. Wählen Sie aus dem Kontextmenü zu diesem Eintrag „Anhalten“ aus.

4.3 Fachliche Anwendungsfälle

4.3.1 Der schnelle Weg: Erstregistrierung einer E-Mail-Adresse mittels T-Wizard

Der T-Wizard ermöglich Ihnen, assistenzgestützt eine erste E-Mail-Adresse zu registrieren.

Wichtiger Hinweis: Die Erstregistrierung einer E-Mail-Adresse mittels T-Wizard eignet sich für den Einsatz direkt nach einer Installation, da im Laufe der Registrierung auch ein Zertifikatsdownload zum KIM-Client erfolgt. Handelt es sich nicht um eine Erstregistrierung, dann sollten Sie die Verwaltung (Admin-Client) zur Registrierung verwenden. Siehe hierzu Kapitel 4.3.3.2.

Der T-Wizard wird automatisch gestartet, sofern Sie bei der Installation angegeben haben, dass Sie eine KIM-E-Mail-Adresse direkt im Anschluss an die Installation anlegen wollen (siehe hierzu auch Kapitel 3.3.3).

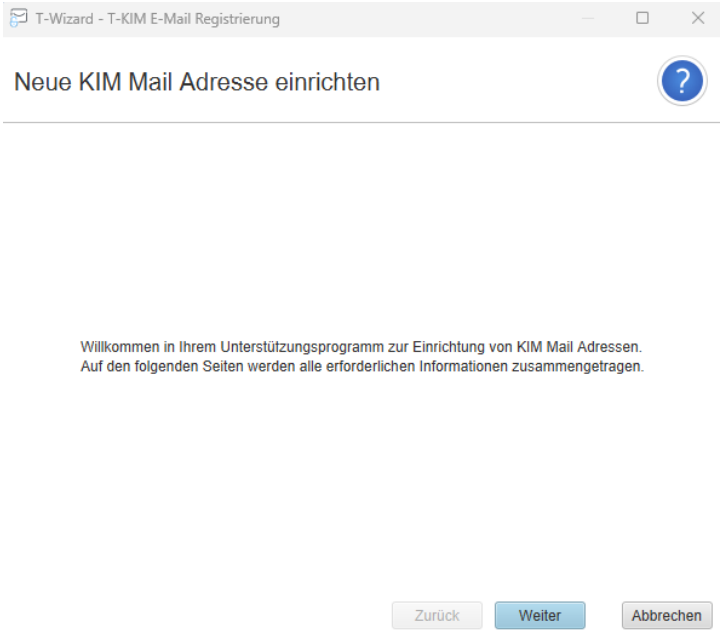

Abbildung 27: T-Wizard – Begrüßungsdialog

Wählen Sie im nächsten Schritt aus, welcher Konnektor verwendet werden soll:

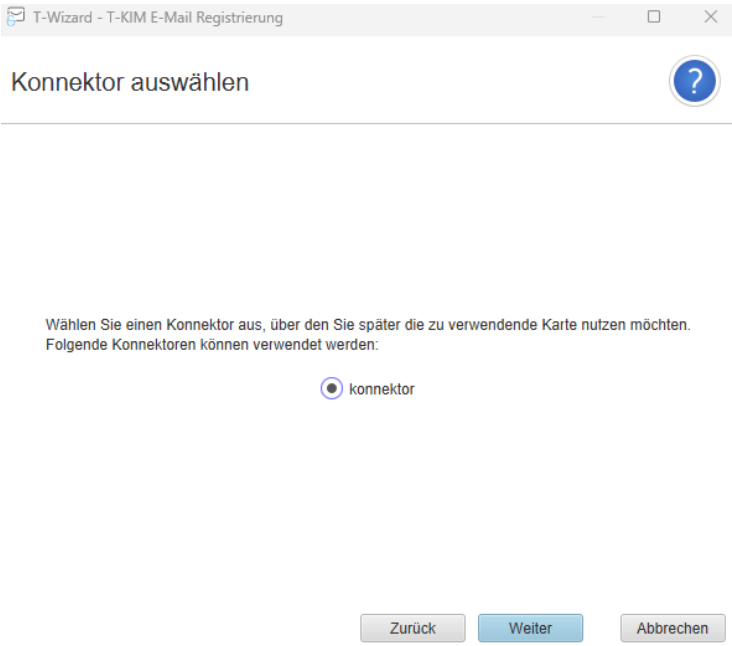

Abbildung 28: T-Wizard – Konnektorauswahl

Wählen Sie den Mandantenkontext aus, den Sie nutzen möchten:

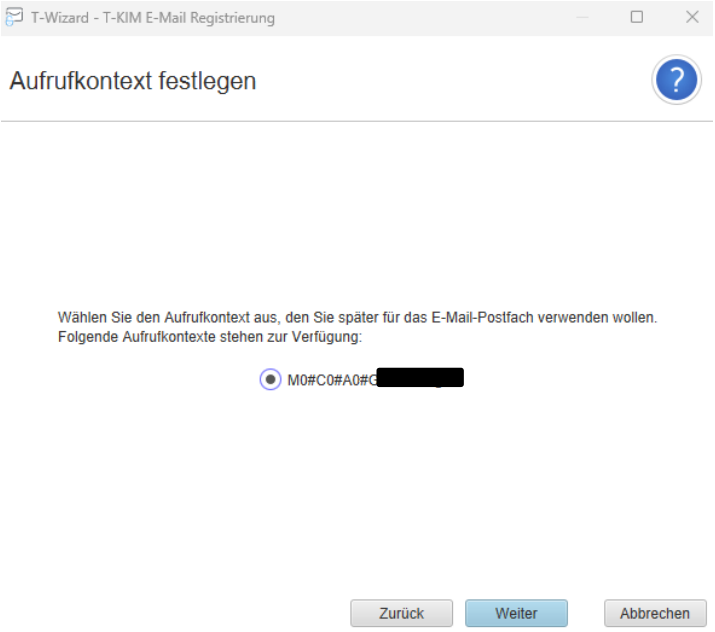

Abbildung 29: T-Wizard – Mandantenkontext

Schließlich wählen Sie eine Karte aus der Liste der angezeigten Karten aus. Diese kann sowohl Institutionskarten als auch Heilberufekarten beinhalten. Sie können die Art der Karten anhand des vor der Bezeichnung stehenden Symbols unterscheiden:

Symbol	Beschreibung
	Personenbezogene Karte (HBA)
	Institutionsbezogene Karte (SMC-B)

Tabelle 2: Symbole für Kartentypen

Wählen Sie die Karte aus, die zukünftig mit dem E-Mail-Konto verwendet werden soll:

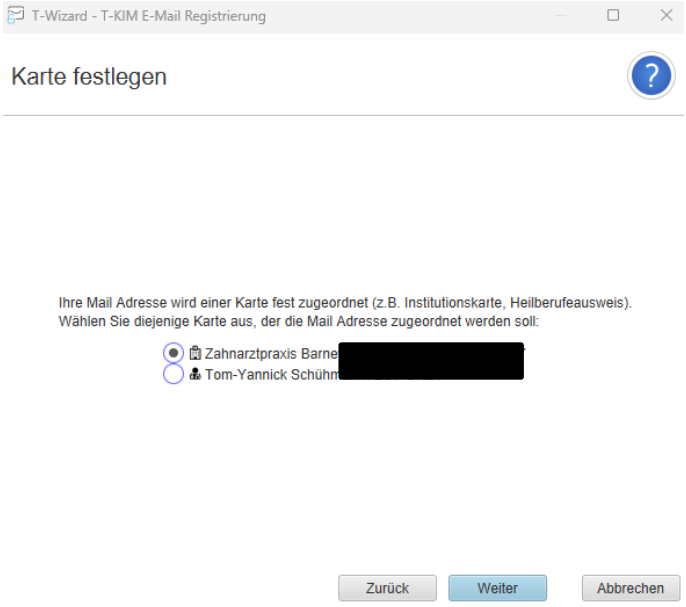

Abbildung 30: T-Wizard – Kartenauswahl

In Abbildung 30 wurde bspw. eine Praxiskarte (SMC-B) ausgewählt.

Bis hierher haben Sie den Karten- und Konnektorkontext konfiguriert. Im nächsten Schritt geht es um die Registrierungsinformationen zur E-Mail-Adresse selbst. Ergänzen Sie dazu den folgenden Dialog:

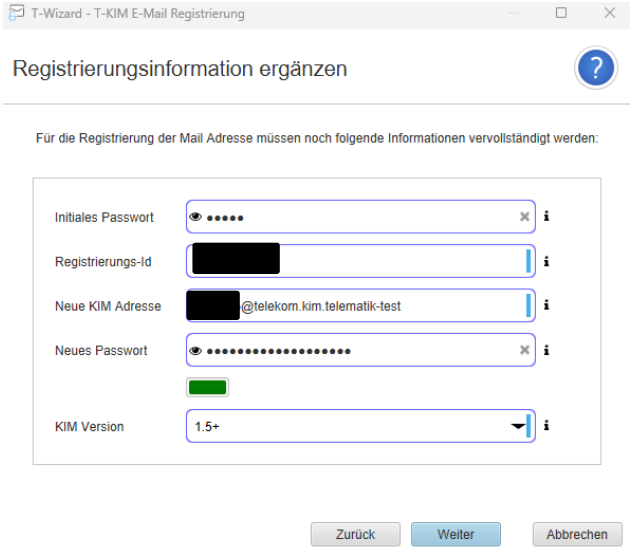

Abbildung 31: T-Wizard – Registrierungsinformationen

- Geben Sie unter „Initiales Passwort“ das Ihnen übermittelte Anfangspasswort ein.
- Geben Sie die Registrierungs-ID an, die Sie im Rahmen der Auftragsbestätigung erhalten haben.
- Wählen Sie Ihre individuelle E-Mail-Adresse. Achten Sie dabei auf die richtige Domäne. Beachten Sie die Bildungsregeln für gültige E-Mail-Adressen in Kapitel 4.1.2.
- Vergeben Sie ein gültiges Passwort. Eine Übersicht der Passwortregeln erhalten Sie in Kapitel „4.1.1 Regeln zur Bildung von Kennwörtern“.

- Wiederholen Sie das Passwort.
- Legen Sie fest, welche KIM-Version als Grundlage für Ihr Postfach verwendet werden soll.

  Folgende KIM-Versionen stehen zur Verfügung:

  - KIM 1.0 – Standardimplementierung
  - KIM 1.5 – ermöglicht die Übertragung großer Anhänge[3]
  - KIM 1.5+ - Bereitschaftssignalisierung für Empfang großer Nachrichten[4]

Nach Eingabe aller Daten drücken Sie auf „Weiter“.

Sie gelangen dann in die Zusammenfassungsansicht:

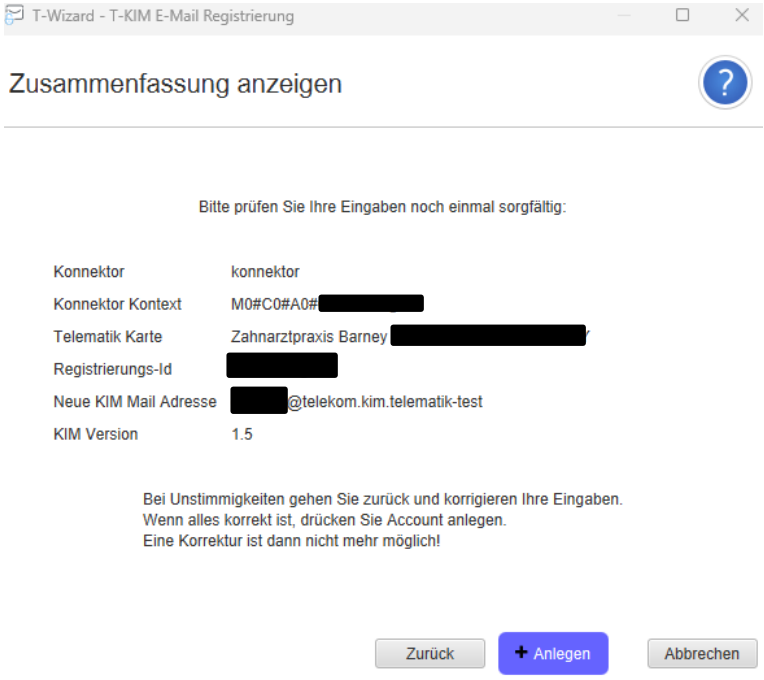

Abbildung 32: T-Wizard – Zusammenfassung anzeigen

Prüfen Sie alle von Ihnen eingegebenen Daten noch einmal sorgfältig.

Drücken Sie als nächstes auf „Anlegen“.

„Anlegen“ bewirkt, dass alle erforderlichen Konfigurationsinformationen auf die Systeme (Lokal, Fachdienst KIM, Verzeichnisdienst-TI) übertragen werden und damit die E-Mail-Adresse registriert wird.

Nach erfolgreicher Registrierung erhalten Sie die Meldung „Der neue Account wurde erfolgreich angelegt.“.

---

[3] Der Fachdienst muss die Übertragung großer Anhänge unterstützen. Diese Einstellung wird auf dem VZD der TI gespeichert. Mit der Einstellung 1.5 signalisieren Sie dem sendenden System, dass Sie bereits Version 1.5 unterstützen.

[4] Die Bereitschaftssignalisierung entspricht einem Opt-In in das Empfangen großer Nachrichten.

Drücken Sie nach dem Anlegen auf „Weiter“. Im Folgedialog installieren Sie ein Sicherheitszertifikat.

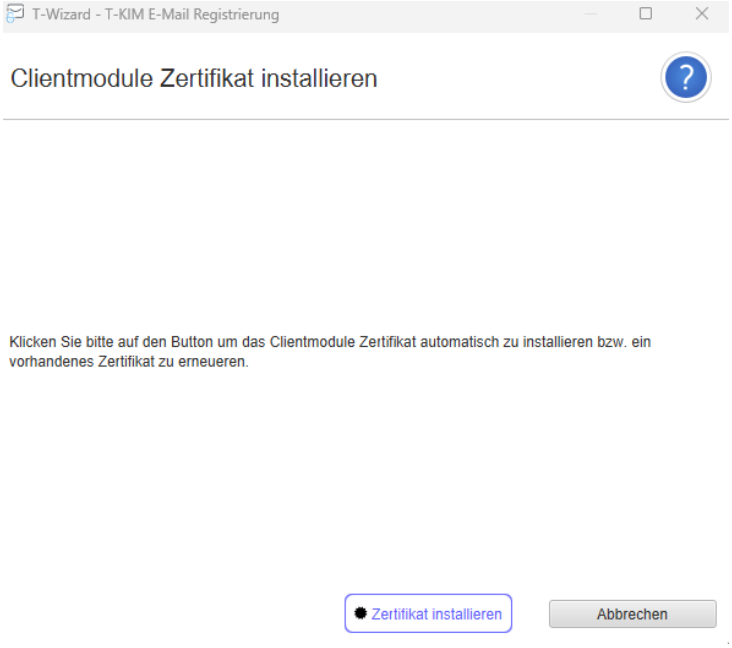

Abbildung 33: T-Wizard – Zertifikat installieren

Dieses Sicherheitszertifikat ist erforderlich, um sich mit dem Fachdienst verbinden zu können. Es kann weiterhin für die Verschlüsselung (TLS) zum E-Mail-Client und dem Konnektor verwendet werden.

Wichtiger Hinweis: Verwenden Sie „Zertifikat installieren“ ausschließlich, wenn dies die erste Registrierung einer E-Mail-Adresse auf dem Installationsrechner ist. Wenn Sie bereits eine bestehende Installation nutzen und Sie ausschließlich eine neue E-Mail-Adresse anlegen wollen, drücken Sie „Abbrechen“. Das vorhandene Zertifikat wird dann weiterhin genutzt.

Nach dem Drücken des Buttons „Zertifikat installieren“ wird dieses im KIM-Client installiert. Drücken Sie dann den Button „Weiter“ um in den letzten Dialog des Assistenten zu gelangen:

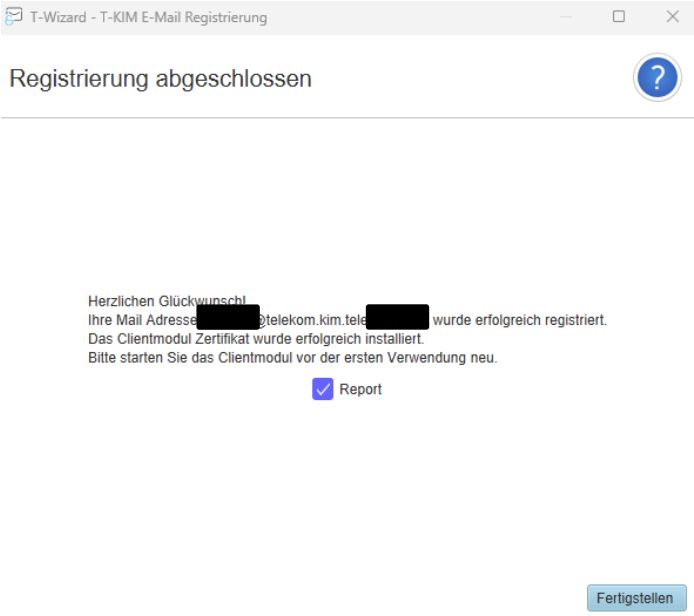

Abbildung 34: T-Wizard – Registrierung abschließen

Die Registrierung ist mit Erreichen dieses Dialogs bereits abgeschlossen. Sie haben nun noch die Möglichkeit, sich einen Report generieren zu lassen, den Sie dann ausdrucken und sicher verwahren können.

Der Report beinhaltet u.a.

- Informationen zu KIM, wie E-Mail-Adresse, zugehörige RegID sowie die konfigurierte KIM-Version
- Lokale Clientsystem-Informationen
- Vollständigen Benutzername zum direkten Übernehmen in einen E-Mail-Client
- Konnektorinformationen
- Verwendeten Mandantenkontext
- Karteninformationen

Damit ist der Registrierungsvorgang beendet.

Wichtiger Hinweis:

Bitte verzichten Sie im Rahmen der Nutzung Ihrer KIM-E-Mail-Adresse auf die Verwendung der bcc-Funktionalität (blind-carbon-copy) Ihres E-Mail-Clients. Es kann technisch nicht ausgeschlossen werden, dass Nachrichtenempfänger ggf. auch alle bcc-Empfänger der Nachricht ermittelt werden können.

4.3.2 Verwendung des Zertifikatsdownloads

Sofern Sie für eine Neuinstallation lediglich eine neues Clientzertifikat benötigen, können Sie dieses über den Zertifikatsdownload erhalten.

Der Zertifikatsdownload startet im Allgemeinen automatisch, nach einer Neuinstallation.

Der Assistent beginnt mit einem Willkommensdialog:

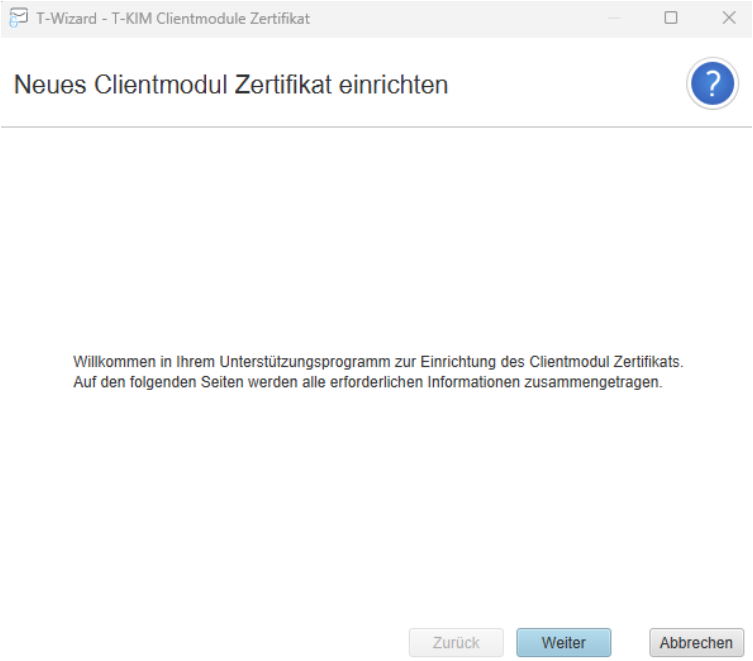

Abbildung 35: Zertifikatsdownload – Willkommensdialog

Drücken Sie auf „Weiter“, um in den nächsten Dialog zu gelangen:

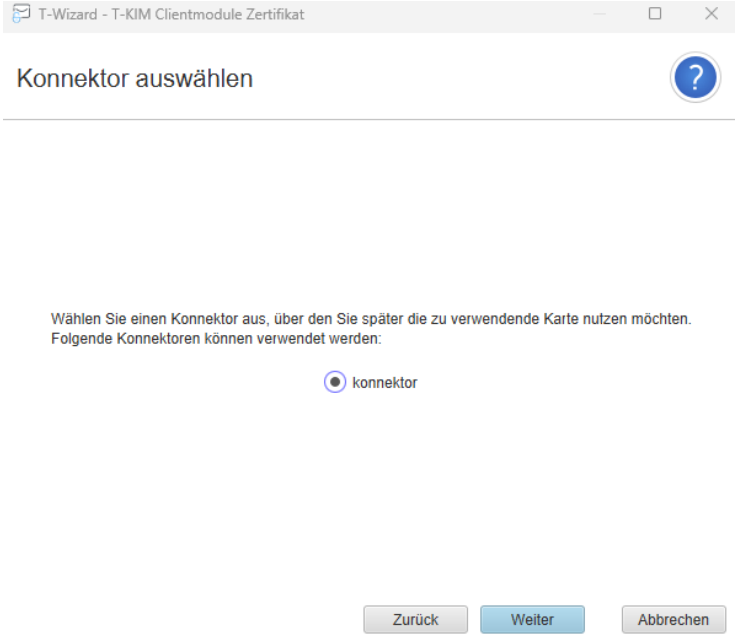

Abbildung 36: Zertifikatsdownlod – Konnektor-Auswahl

Wählen Sie hier den zu verwendenden Konnektor aus und drücken dann auf „Weiter“.

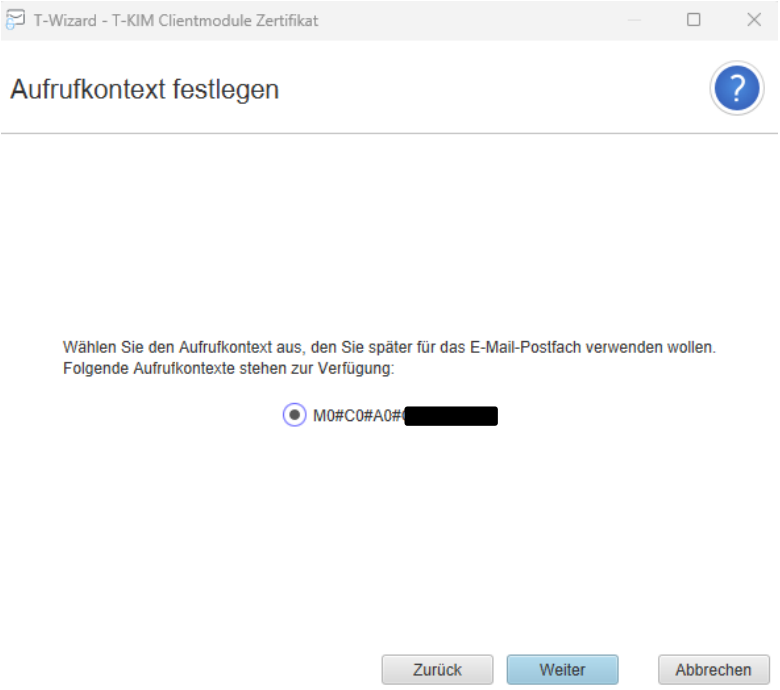

Abbildung 37: Zertifikatsdownload – Aufrufkontext festlegen

Legen Sie den zu verwendenden Aufrufkontext fest und drücken dann „Weiter“.

Der Aufruf der nächsten Seite kann etwas dauern, da der Assistent alle unter dem Aufrufkontext verfügbaren Karten ermittelt.

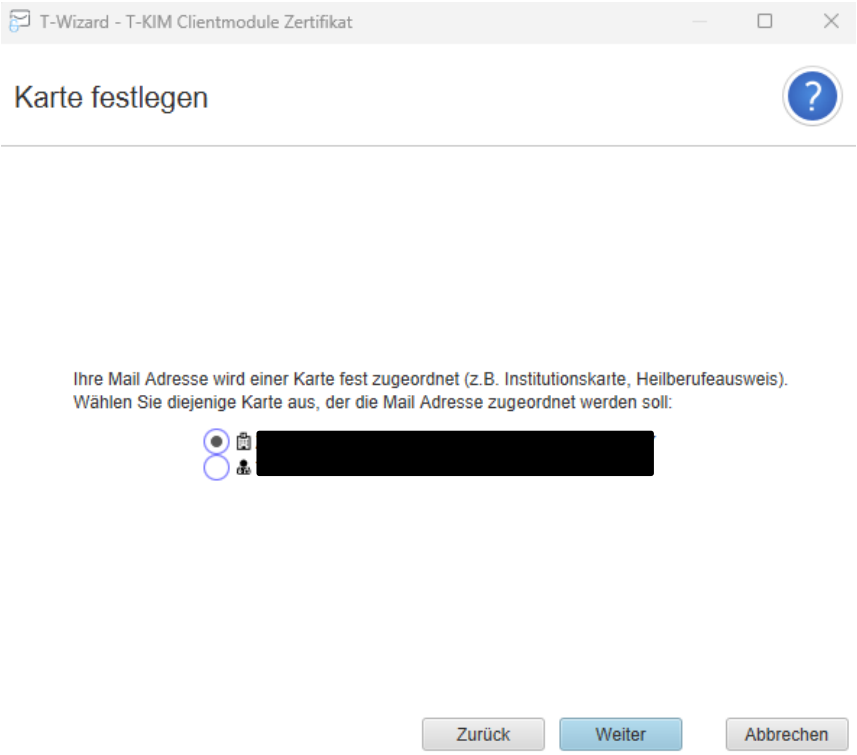

Abbildung 38: Zertifikatsdownload – Karte festlegen

Wählen Sie eine Karte aus und drücken dann „Weiter“.

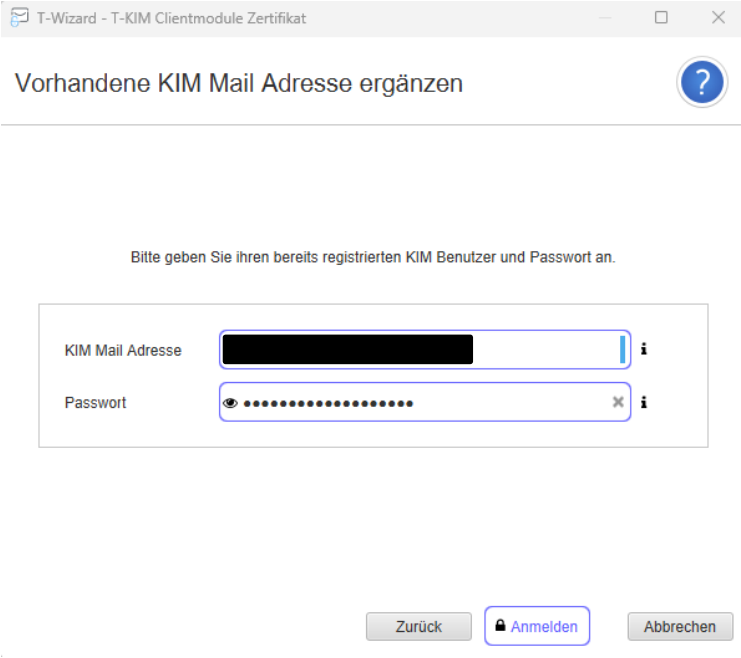

Abbildung 39: Zertifikatsdownload – Vorhandene KIM-Mail-Adresse ergänzen

Geben Sie hier die bereits registrierte E-Mail-Adresse ein. Drücken Sie danach auf Weiter.

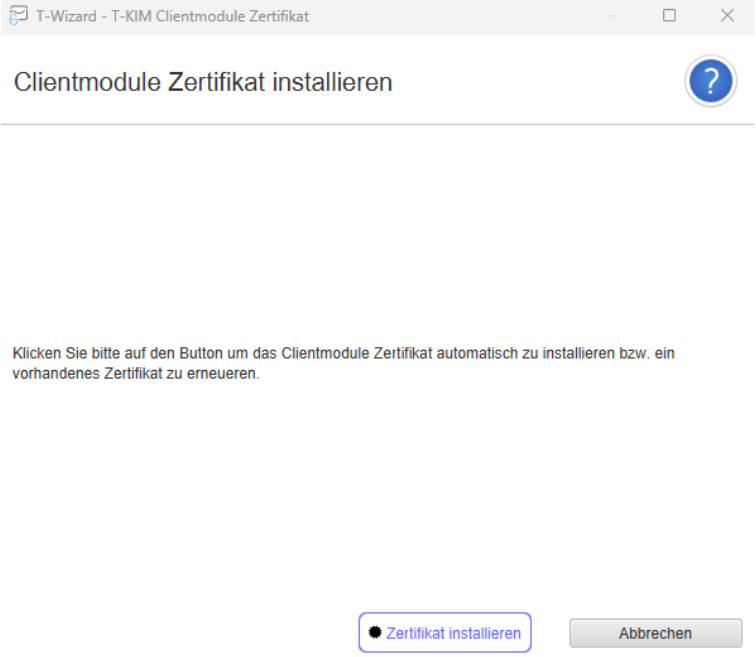

Abbildung 40: Zertifikatsdownload – Zertifikat installieren

Wenn Sie „Zertifikat installieren“ drücken, wird mit Ihren Angaben in der TI eine Clientzertifikat erstellt, dass auf den Installationsrechner ausgestellt ist. Dieses Zertifikat gilt ausschließlich für diesen Rechnernamen.

Damit ist die Installation des Clientzertifikats abgeschlossen:

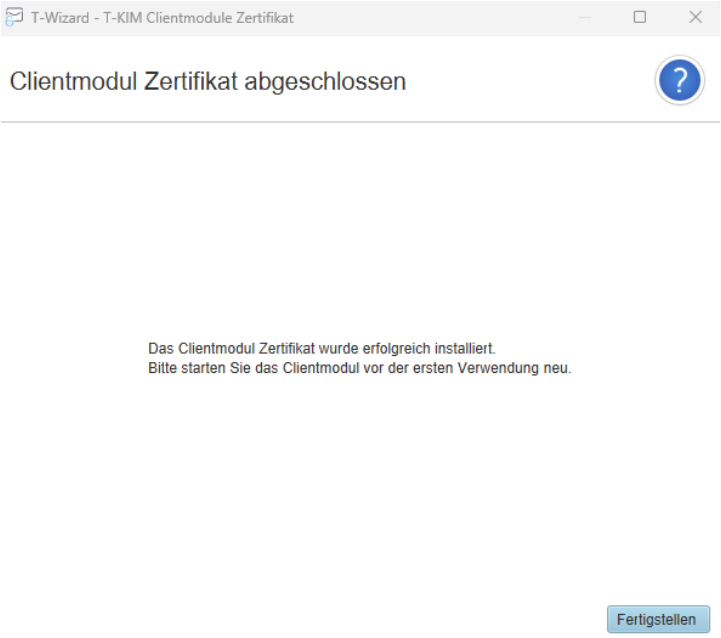

Abbildung 41: Zertifikatsdownload – Clientmodul-Zertifikat abgeschlossen.

Mit Drücken auf „Fertigstellen“ beenden Sie den Assistenten.

4.3.3 Nutzung der Verwaltung

4.3.3.1 Aufruf der Verwaltung

Die Verwaltung kapselt alle Funktionalitäten rund um die Administration von E-Mail-Konten. Es ist der zentrale Einstiegspunkt des KIM-Clients. Über die Verwaltung können Sie folgende Aufgaben erledigen:

- E-Mail-Account anlegen (Kapitel 4.3.3.2)
- E-Mail-Account bearbeiten (Kapitel 4.3.3.3)
- Übersicht aller registrierten E-Mail-Accounts zu einer Telematikkarte anzeigen (Kapitel 4.3.3.3)
- Verzeichnisdienstabfrage zu Basis- und Fachdaten sowie detaillierte Zertifikatsinformationen (Kapitel 4.3.3.9)
- Selbsttest und Erreichbarkeitstest Fachdienst durchführen (Kapitel 4.3.3.5)
- Software-Update (Kapitel 4.3.3.9.9)
- Zertifikatsdetails zum Clientzertifikat abrufen (Kapitel 4.3.3.9.12)
- Zertifikatsinformationen zu einer Telematikkarte abrufen (Kapitel 4.3.3.9.11)
- Metriken abrufen (Kapitel 4.3.4)
- Unterstützung und Support (Kapitel 4.3.5)
- Allgemeine Einstellungen (Kapitel 4.3.5.4)

Zum Aufruf der Verwaltung gehen Sie folgendermaßen vor:

- Wählen Sie den KIM-Client aus den Symbolen des Windows-Desktop-Trays unten rechts aus. Ggf. ist es erforderlich auch die ausgeblendeten Symbole anzuzeigen.
- Gehen Sie mit dem Mauszeiger über das Symbol des KIM-Clients.
- Drücken Sie die rechte Maustaste.
- Wählen Sie „Verwaltung“ aus.

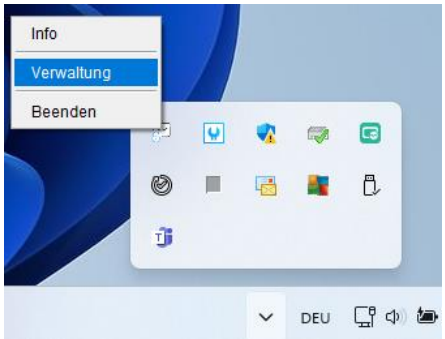

Abbildung 42: Desktop – KIM-Client – Verwaltung

Alternativ rufen Sie die Verwaltung über das Startmenü→T-System-KIM-Clientmodul→T-KIM-Admin-Client auf.

Danach öffnet sich die Verwaltungsansicht. Diese ist dreigeteilt:

- Menüleiste
- Konnektor-Einstellungen
- Account-Ansicht

Die einzelnen Funktionen, die Sie ausführen können, sind in den nachfolgenden Kapiteln beschrieben.

4.3.3.2 E-Mail-Account anlegen

Das Anlegen eines E-Mail-Kontos erfordert die Angabe der Konnektor-Einstellungen.

Um ein E-Mail-Konto anzulegen, wählen Sie daher

- den Konnektor aus, der verwendet werden soll,
- den Mandantenkontext, der im Kontext des Konnektors aufgerufen werden soll und
- die Telematikkarte, deren Zertifikate für die kryptographischen Funktionen genutzt werden soll.

Hinweis:
Bitte beachten Sie, dass der Konnektor dem entsprechend vorbereitet sein muss.

Drücken Sie dann den Button „Account anlegen“.

Abbildung 43: Verwaltung - Button „Account anlegen“

Im unteren Bereich können sie nun ein E-Mail-Account anlegen.

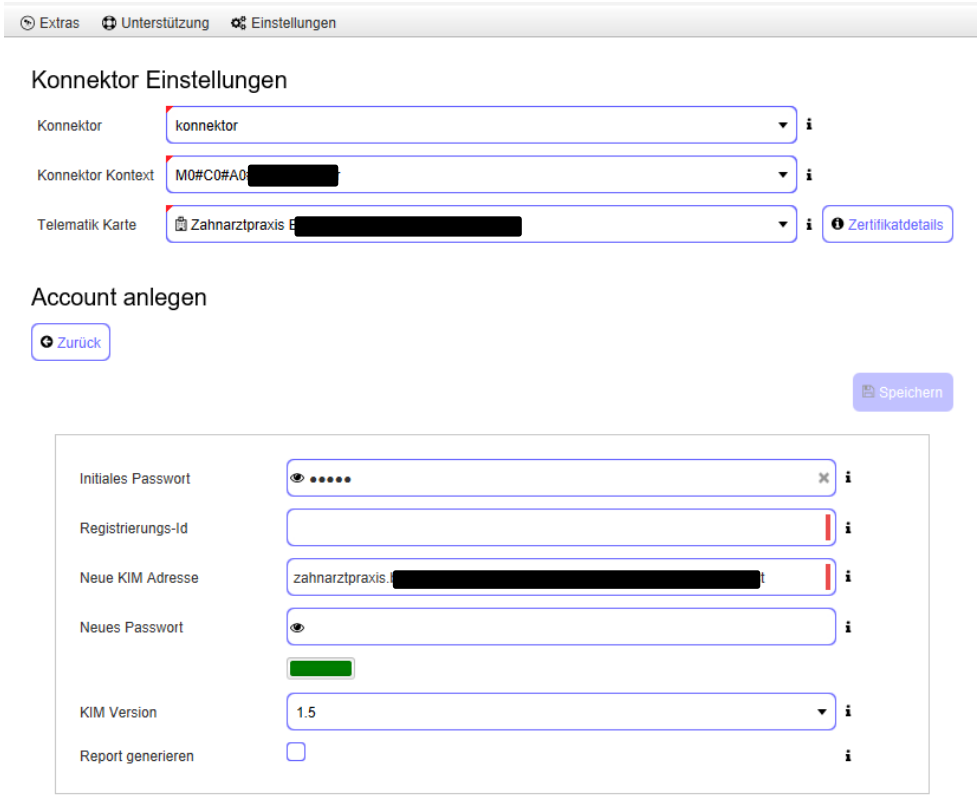

Abbildung 44: KIM-Client – Verwaltungsansicht – Account anlegen

Tragen Sie die erforderlichen Informationen ein.

- Geben Sie unter „Initiales Passwort“ das Ihnen übermittelte Anfangspasswort ein. Sofern der Wert vorbelegt ist, ändern Sie ihn nicht.
- Geben Sie die Registrierungs-ID an, die Sie im Rahmen der Auftragsbestätigung erhalten haben.

- Wählen Sie Ihre individuelle E-Mail-Adresse. Achten Sie dabei auf die richtige Domäne. Beachten Sie die Bildungsregeln für gültige E-Mail-Adressen in Kapitel 4.1.2.
- Vergeben Sie ein gültiges Passwort. Eine Übersicht der Passwortregeln erhalten Sie in Kapitel „4.1.1 Regeln zur Bildung von Kennwörtern“.
- Legen Sie fest, welche KIM-Version als Grundlage für Ihr Postfach verwendet werden soll.

Folgende KIM-Versionen stehen zur Verfügung:

- KIM 1.0 – Standardimplementierung
- KIM 1.5 – ermöglicht die Übertragung großer Anhänge[5]
- KIM 1.5+ - bietet ein Opt-In-Verfahren ergänzend zu KIM 1.5.

Drücken Sie abschließend den Button „Speichern“ um die E-Mail-Adresse zu prüfen und anlegen zu lassen. Sofern die Checkbox „Report generieren“ gesetzt ist, wird Ihnen mittels „Speichern unter“-Dialog die Möglichkeit des Speicherns einer Übersichtsseite zum E-Mail-Account gegeben (siehe hierzu auch unter 4.3.3.4.4).

Wichtiger Hinweis:

Bitte verzichten Sie im Rahmen der Nutzung Ihrer KIM-E-Mail-Adresse auf die Verwendung der bcc-Funktionalität (blind-carbon-copy) Ihres E-Mail-Clients. Es kann technisch nicht ausgeschlossen werden, dass Nachrichtenempfänger ggf. auch alle bcc-Empfänger der Nachricht ermittelt werden können.

4.3.3.3 Account-Ansicht (E-Mail-Übersicht)

Die Übersicht der E-Mail-Konten erfordert die Angabe der Konnektoreinstellungen.

Um die Kontenübersicht zu erhalten, wählen Sie daher

- den Konnektor aus, der verwendet werden soll,
- den Mandantenkontext, der im Kontext des Konnektors aufgerufen werden soll und
- die Telematikkarte, deren Zertifikate für die kryptographischen Funktionen genutzt werden soll.

Mit Auswahl der Telematikkarte wird die Account-Ansicht im unteren Bereich der Verwaltung aufgelistet:

[5] Der Fachdienst muss die Übertragung großer Anhänge unterstützen. Diese Einstellung wird auf dem VZD der TI gespeichert. Mit der Einstellung 1.5 signalisieren Sie dem sendenden System, dass Sie bereits Version 1.5 unterstützen.

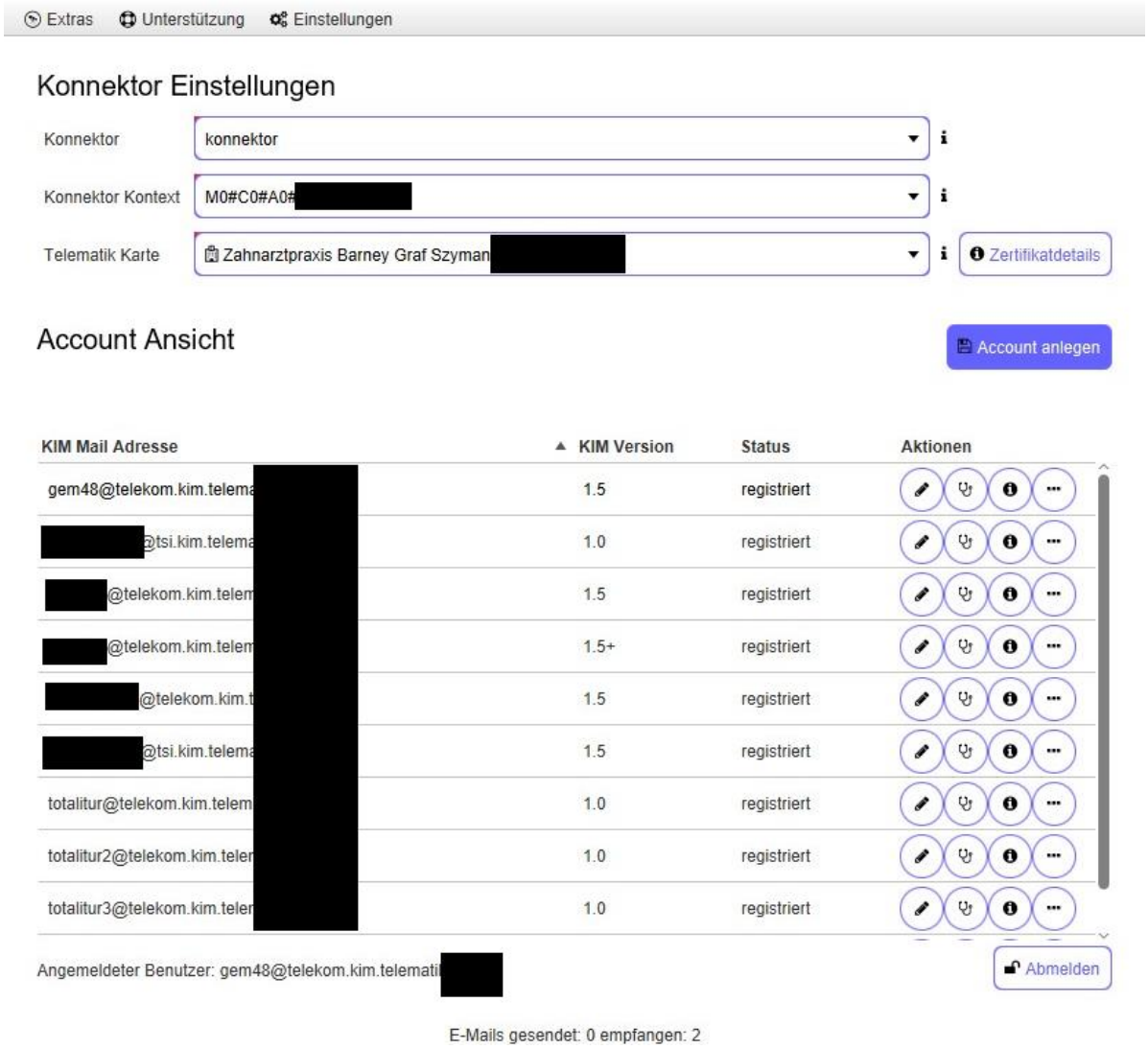

Abbildung 45: Admin-Client mit Account-Ansicht

Ergänzend zur Auflistung der E-Mail-Accounts erhalten Sie auch eine erste Information bzgl. KIM-Version und Status für jedes einzelne Konto dargestellt.

4.3.3.4 E-Mail-Account bearbeiten

4.3.3.4.1 Vorbemerkung

Das Bearbeiten eines E-Mail-Kontos erfordert die Angabe der Konnektor-Einstellungen.

Um ein E-Mail-Konto bearbeiten zu können, wählen Sie aus der Account-Ansicht die zu bearbeitende Adresse aus und drücken auf den Aktionsbutton „Einen Datensatz bearbeiten“.

Abbildung 46: Account-Ansicht – Aktionsbutton „Einen Datensatz bearbeiten“

Die Bearbeitung erfordert ggf. eine Passworteingabe. Drücken Sie dann den „Anmelden-Button“.

Nach erfolgreicher Anmeldung können Sie nun die Bearbeitung vornehmen.

4.3.3.4.2 Passwort ändern

Bitte beachten Sie die Vorbemerkungen in Kapitel 4.3.3.4.1.

- Wechseln Sie sofern noch nicht geschehen in die Ansicht „Account bearbeiten“.
- Geben Sie ein neues Kennwort ein und bestätigen Sie es. Beachten Sie dabei die Kennwortregeln.
- Drücken Sie den Button „Speichern“.

Das neue Kennwort wird sodann gespeichert.

Wichtiger Hinweis:

Bitte denken Sie daran, dass das neue Kennwort auch in Ihrem E-Mail-Client geändert werden muss, da Sie sonst dort keinen Zugriff auf das Postfach bekommen.

4.3.3.4.3 KIM-Version einstellen

Bitte beachten Sie die Vorbemerkungen in Kapitel 4.3.3.4.1.

- Wechseln Sie sofern noch nicht geschehen in die Ansicht „Account bearbeiten“.
- Wählen Sie aus der Dropdown-Box die entsprechende Version[6] aus.
- Drücken Sie den Button „Speichern“.

Folgende KIM-Versionen stehen zur Verfügung:

Version	Senden	Empfangen	Anmerkung
KIM 1.0	< 15 MiB	< 15 MiB	Standardimplementierung
KIM 1.5	> 15 MiB	< 15 MiB	Ermöglicht das Senden großer Mails, der Empfang ist beschränkt
KIM 1.5+	> 15 MiB	> 15 MiB	Senden und empfangen großer Mails möglich

Tabelle 3: Übersicht KIM-Versionen

[6] Der Fachdienst unterstützt bereits die Übertragung großer Anhänge. Diese Einstellung wird auf dem VZD der TI gespeichert. Mit der Einstellung 1.5 signalisieren Sie dem sendenden System, dass Sie bereits Version 1.5 unterstützen.

Hinweis:

Sofern Sie „KIM 1.5+“ ausgewählt haben, werden Sie auf Systemvoraussetzungen hingewiesen.

KIM 1.5+ kann evtl. auch dann verwendet werden, wenn die Systemvoraussetzungen nicht bzw. nicht vollständig erfüllt werden. Dies kann aber zu Einbußen bzgl. Performance oder instabilem Verhalten führen.

Die KIM-Version wird im Verzeichnisdienst angepasst.

4.3.3.4.4 Report generieren

Bitte beachten Sie die Vorbemerkungen in Kapitel 4.3.3.4.1.

- Wechseln Sie sofern noch nicht geschehen in die Ansicht „Account bearbeiten“.
- Setzen Sie bei „Report generieren“ ein Häkchen.
- Drücken Sie den Button „Speichern“.

Der Report umfasst die aktuelle Konfiguration des E-Mail-Accounts. Sie können ihn als PDF-Datei speichern.

Wichtiger Hinweis:

Da der Report sensible Informationen enthält, sollten Sie ihn an einem sicheren Ort verwahren!

4.3.3.5 Selbsttest

Den Selbsttest finden Sie hier:

- Wechseln Sie sofern noch nicht geschehen in die „Account-Ansicht“.
- Drücken Sie den Aktionsbutton „Selbsttest starten“.

Abbildung 47: Erweiterte Funktionen - Selbsttest

Der KIM-Admin-Client wechselt zur Ansicht „Selbsttest“.

Zur Durchführung des Selbsttest drücken Sie den Button „Selbsttest starten“. Der Test erfolgt automatisch.

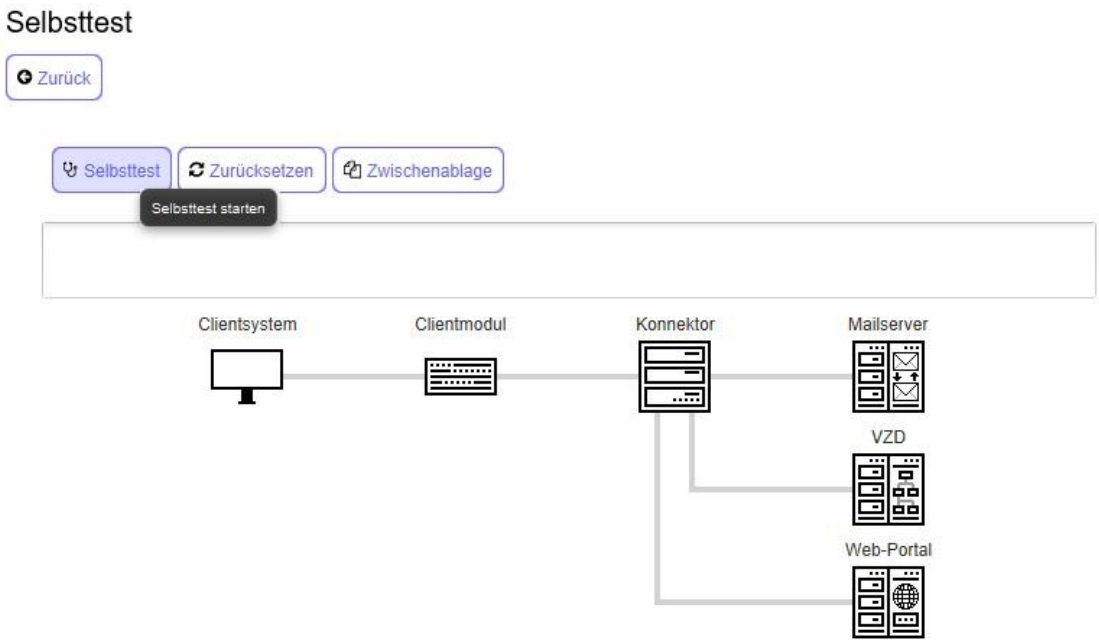

Abbildung 48: KIM-Client – Selbsttest

Der Selbsttest prüft die Erreichbarkeit zu Konnektor, Mailserver, VZD und Webportal.

Sofern alle Testschritte erfolgreich durchgeführt werden konnten, wird Ihnen dies zum einen als Protokoll, zum anderen visuell in „Grün“ dargestellt.

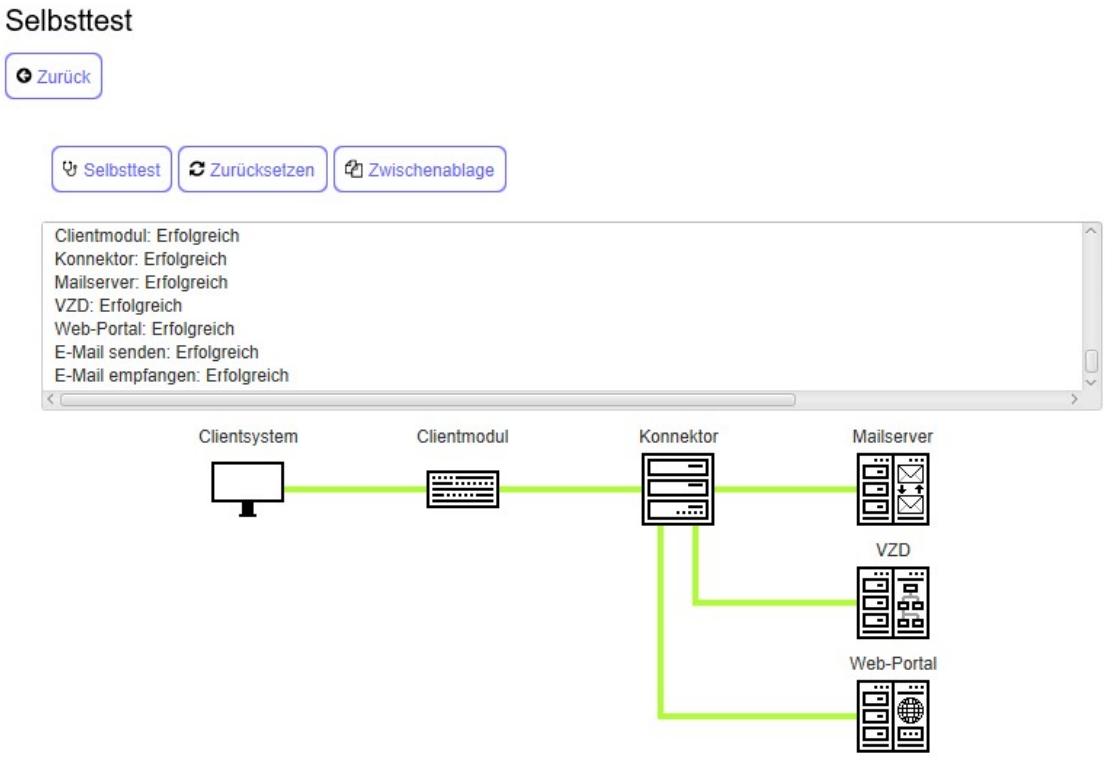

Abbildung 49: KIM-Client – Selbsttest erfolgreich

Die Protokollansicht zeigt ihnen, bei welchem Testschritt ein Fehler aufgetreten ist. Die davon betroffene Strecke wird dann in „Rot“ ausgewiesen.

4.3.3.6 E-Mail-Account deregistrieren

ACHTUNG!

Das Deregistrieren eines E-Mail-Accounts hat zur Folge, dass über das Konto keine Mails mehr gesendet oder empfangen werden können.

Sie können noch 30 Tage lang auf die Nachrichten des Postfachs zugreifen. Danach wird das Postfach und alle enthaltenen Mails permanent gelöscht.

Sofern die Deregistrierung unbeabsichtigt war, können Sie diese in einem Zeitraum von 30 Tagen nach der Deregistrierung am Webportal rückgängig machen.

So gelangen Sie zur Deregistrierung:

- Wechseln Sie sofern noch nicht geschehen in die „Account-Ansicht“.
- Drücken Sie den Aktionsbutton „Erweiterte Funktionen“ (Drei-Punkte-Button).
- Klicken Sie auf „Deregistrierung“.

Abbildung 50: Erweiterte Funktionen - Deregistrierung

Es wird ein Sicherheitshinweis zu den Folgen der Deregistrierung angezeigt. Sie können zu diesem Zeitpunkt die Deregistrierung durch Drücken auf „Abbrechen“ die Deregistrierung noch verwerfen.

Mit Drücken auf „OK“ wird die Deregistrierung ausgeführt.

Das Konto wird danach deregistriert und steht Ihnen nicht mehr zum Senden und Empfangen zur Verfügung.

4.3.3.7 E-Mail-Account reaktivieren

Es können nur deregistrierte Konten reaktiviert werden.

Um ein deregistriertes Konto zu reaktivieren, gehen Sie folgendermaßen vor:

- Wechseln Sie sofern noch nicht geschehen in die „Account-Ansicht“.
- Drücken Sie den Aktionsbutton „Erweiterte Funktionen“ (Drei-Punkte-Button).
- Klicken Sie auf „Reaktivieren“.

Abbildung 51: Erweiterte Funktionen - Reaktivierung

Überdies können Sie das Konto auch über das Webportal reaktivieren. Bitte loggen Sie sich hierzu am Webportal mit den entsprechenden Anmeldeinformationen innerhalb von 30 Tagen nach Deregistrierung ein, um das E-Mail-Konto zu reaktivieren.

4.3.3.8 Zertifikat installieren

- Wechseln Sie sofern noch nicht geschehen in die „Account-Ansicht“.
- Drücken Sie den Aktionsbutton „Erweiterte Funktionen“ (Drei-Punkte-Button).
- Klicken Sie auf „Zertifikat installieren“.

Abbildung 52: Erweiterte Funktionen – Zertifikat installieren

Die Funktion sollten Sie dazu benutzen, das KIM-Client-Zertifikat kurz vor Ablauf der Gültigkeitsdauer zu ersetzen.

Bitte beachten Sie, dass Sie dieses Zertifikat auch ggf. im Rahmen von TLS an Ihrem E-Mail-Client neu konfigurieren müssen.

4.3.3.9 Verzeichnisdienstfunktionalität

4.3.3.9.1 Vorbemerkung

Um den Verzeichnisdienst abzufragen, führen Sie diese Schritte aus:

- Wechseln Sie sofern noch nicht geschehen in die „Account-Ansicht“.
- Wählen Sie das Konto aus, zu dem Sie die Abfrage stellen wollen.
- Drücken Sie den Aktionsbutton „Erweiterte Funktionen“ (Drei-Punkte-Button).

- Klicken Sie auf „VZD“.

Abbildung 53: Erweiterte Funktionen - VZD

Sie erreichen die Übersicht zum Basiseintrag, des ausgewählten Kontos.

Hinweis: Diesem Basiseintrag können auch weitere E-Mail-Konten zugeordnet sein.

Im oberen Teil der Ansicht können Sie den LDAP-Kontext wählen und den PKI-Cache leeren.

Die Übersicht enthält auch drei Reiter:

- Fachdaten: Übersicht der KIM-Mail-Adressen und deren Version
- Basisdaten: Informationen zur zugrundeliegenden Karte (SMC-B oder HBA)
- Zertifikat: Öffentlich verfügbare Informationen zum Zertifikat der zugrundeliegenden Karte.

In den nachfolgenden Kapiteln werden Sie durch die Funktionalität der Verzeichnisdienstabfrage geführt.

4.3.3.9.2 Fachdaten abrufen

Wählen Sie den Tab „Fachdaten“ aus, um die verfügbaren Fachdaten zur angegebenen Telematikkarte abzurufen:

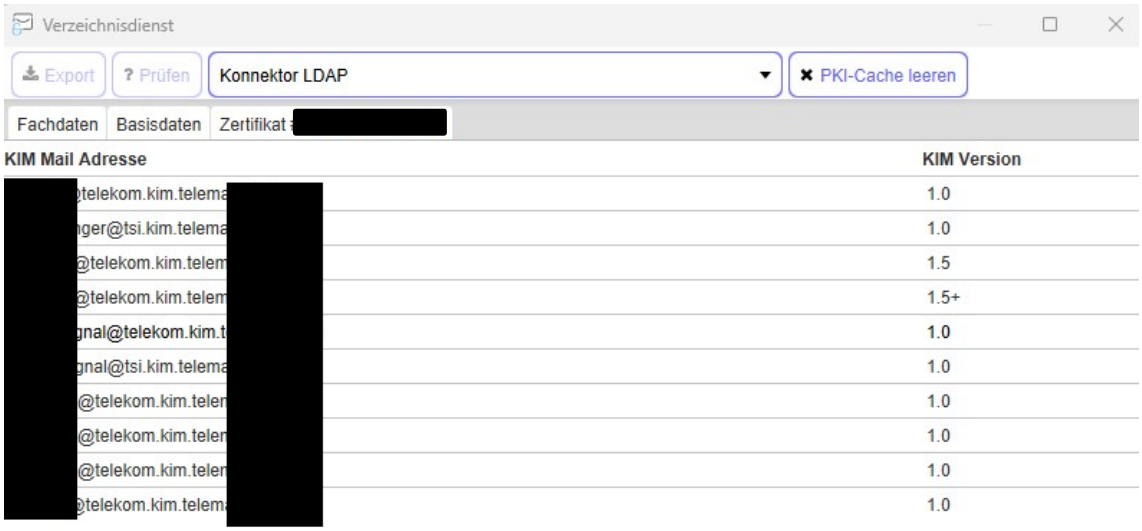

Abbildung 54: KIM-Client – Fachdaten aus Verzeichnisdienst

Sie erhalten eine Übersicht zu

- Zugeordnete KIM-E-Mail-Adressen
- Unterstützte KIM-Version je KIM-E-Mail-Adresse

4.3.3.9.3 Basisdaten abrufen

Wählen Sie den Tab „Basisdaten“ aus, um die verfügbaren Basisdaten zur angegebenen Telematikkarte abzurufen:

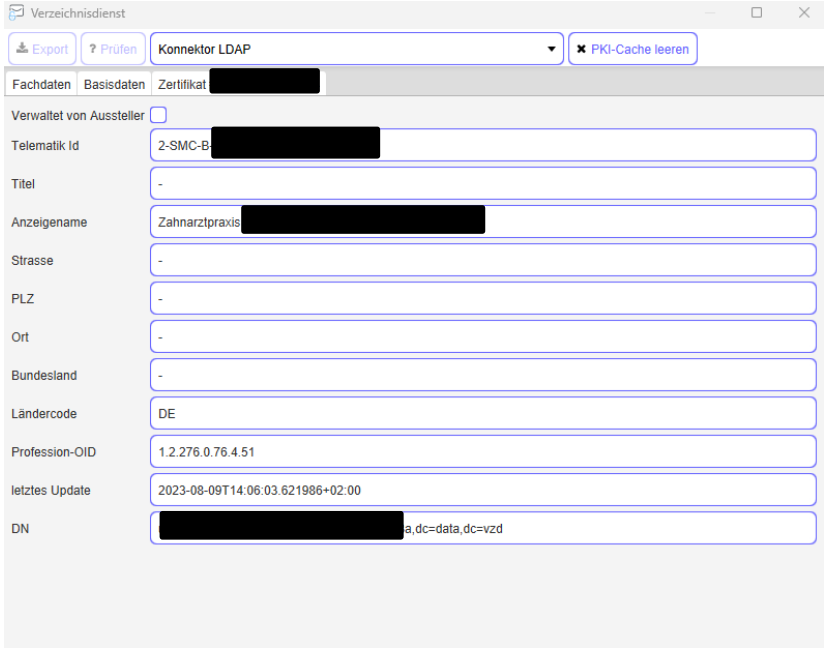

Abbildung 55: KIM-Client – Basisdaten aus Verzeichnisdienst

Sie erhalten hier eine Übersicht der zum Basiseintrag verfügbaren Informationen.

Des Weiteren wird Ihnen angezeigt, ob der Eintrag vom Aussteller verwaltet wird oder nicht.

4.3.3.9.4 Zertifikatsdetails anzeigen

Wählen Sie den Tab „Zertifikat #...“ aus, um Informationen zu einem Zertifikat zu erhalten:

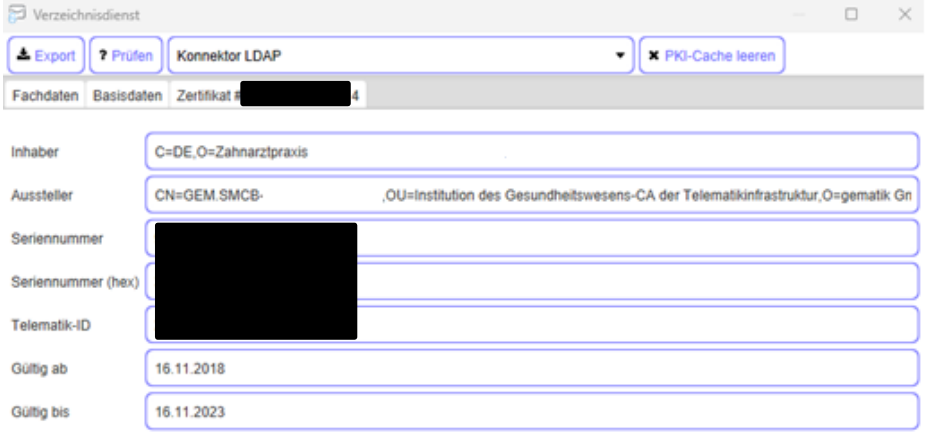

Abbildung 56: KIM-Client – Zertifikatsdetails aus Verzeichnisdienst

4.3.3.9.5 LDAP-Kontext wählen

Der LDAP-Kontext ermöglicht Ihnen, zwischen den lokal gespeicherten Informationen und den auf dem VZD in der TI verfügbaren Informationen zu wechseln, um ggf. Unterschiede zu ermitteln.

Die Wechselmöglichkeit finden Sie in der oberen Mitte des Dialogs:

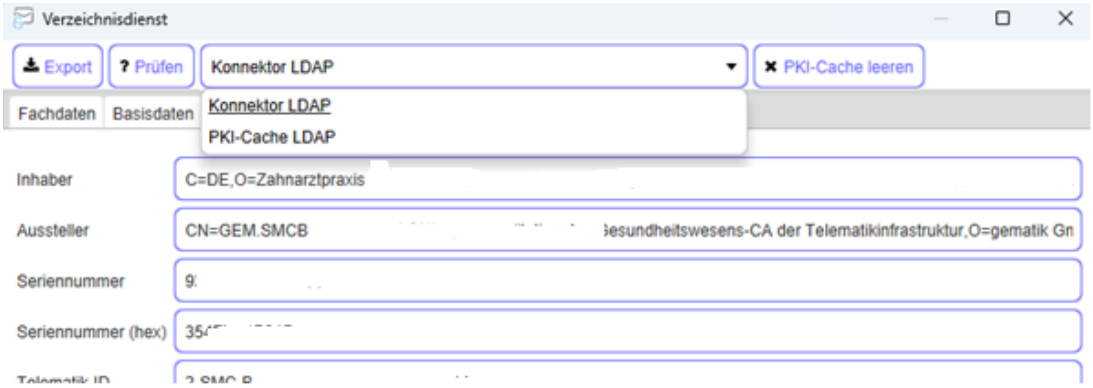

Abbildung 57: KIM-Client – LDAP-Kontext wählen

Für die Sicht auf den VZD wählen Sie „Konnektor-LDAP“ aus. Sofern Sie die lokal gespeicherten Informationen abrufen wollen, wählen sie „PKI-Cache-LDAP“ aus.

4.3.3.9.6 PKI-Cache leeren

Der PKI-Cache ermöglicht Ihnen grundsätzlich, die Anzahl von VZD-Abfragen zu verringern und die Verschlüsselung von Mails zu beschleunigen.

Es kann jedoch auch sinnvoll sein, diesen Cache manuell zu leeren. Um den PKI-Cache zu leeren, drücken Sie auf den Button „PKI-Cache leeren“, der sich oben rechts befindet:

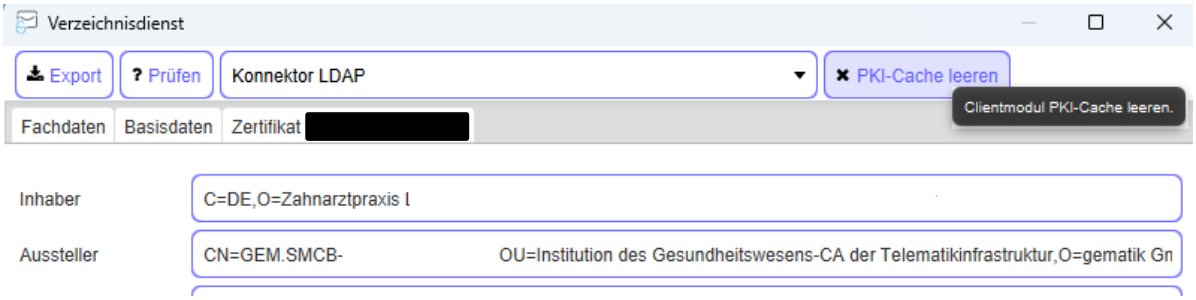

Abbildung 58: KIM-Client – PKI-Cache leeren

4.3.3.9.7 Export des Zertifikats

Über den Button „Export“ können Sie das ausgewählte Zertifikat als crt-Datei exportieren:

- Wählen Sie zunächst den Tab „Zertifikat #…“ aus und drücken dann den Button „Export“.

Es wird ein „Datei speichern unter …“-Fenster geöffnet.

- Wählen Sie das Zielverzeichnis aus, und geben Sie einen Dateinamen an.
- Drücken Sie anschließend „Speichern“.

4.3.3.9.8 Prüfen des Zertifikats

Über den Button „Prüfen“ können Sie das ausgewählte Zertifikat auf Gültigkeit überprüfen lassen:

- Wählen Sie zunächst über den Tab „Zertifikat #...“ das zu prüfende Zertifikat aus und drücken dann den Button „Prüfen“.

Das ausgewählte Zertifikat wird gegen den OCSP-Responder auf Gültigkeit geprüft.

4.3.3.9.9 Mailcache

Der Mailcache ist kein Bestandteil des KIM-Clients. Er gehört zum KIM-Security-Interface und kann optional konfiguriert werden. Zur Konfiguration des Security-Interfaces sei auf dessen Dokumentation verwiesen.

Hinweis: Der Mailcache muss für den KIM-Client aktiviert worden sein, bevor Sie ihn nutzen können. Dies geschieht entweder während der Installation oder aber nachträglich konfigurativ in der clientmodule.xml.

Um den Mailcache für ein Konto zu aktivieren bzw. zu deaktivieren, gehen Sie folgendermaßen vor:

- Wählen sie in der Hauptansicht für das zu konfigurierende Konto die Aktion „Einen Datensatz bearbeiten“.

Zur Verwendung des Mailcaches für dieses Konto setzen Sie den Haken bei „Mailcache aktivieren“. Wenn Sie den Mailcache für das gewählte Konto nicht verwenden wollen, entfernen Sie den Haken.

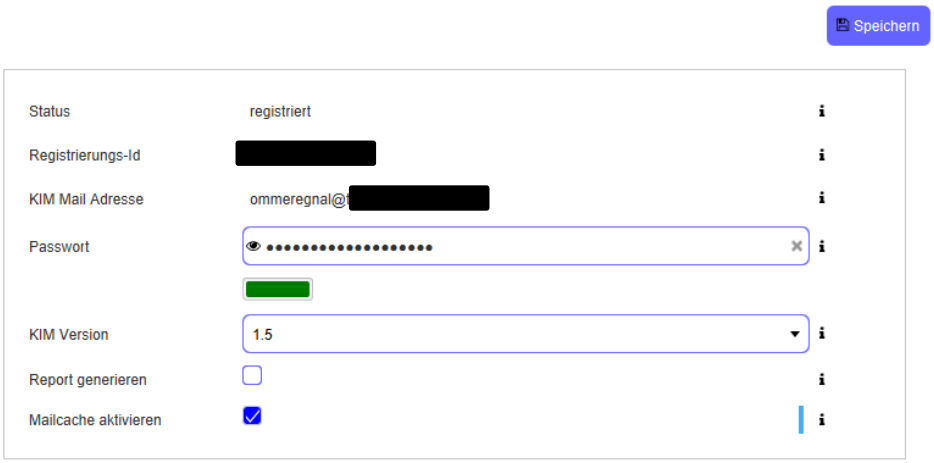

Abbildung 59: KIM-Client – Mailcache

4.3.3.9.10 Software-Updates/Downloads

Software-Updates können Sie folgendermaßen finden:

- Öffnen Sie „Extras“.
- Wählen Sie „Updates“ aus.

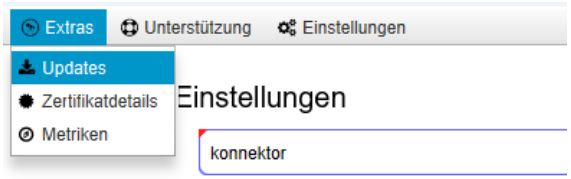

Abbildung 60: KIM-Client – Menü Updates

Die Übersicht sieht folgendermaßen aus:

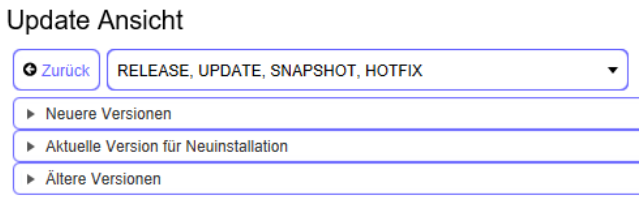

Abbildung 61: KIM-Client - Updates

Diese Ansicht zeigt alle verfügbaren Downloads. Diese sind in Kategorien eingeteilt.

Folgende Kategorien stehen zur Verfügung:

- Release – Vollversion des KIM-Clients
- Update – Aktualisierung, die für eine oder mehrere Releases bereitgestellt wird
- Snapshot – „Zwischenversion“, die zu Testzwecken bereitgestellt wird und nicht ohne Rücksprache eingesetzt werden sollte
- Hotfix – auch Patch genannt, stellt kurzfristig eine Aktualisierung einer bestehenden Version bereit

Des Weiteren können Sie zwischen einer neueren Version, einer aktuellen Version zur Neuinstallation oder einer älteren Version als Downgrade wählen.

Wenn für die entsprechenden Kategorien keine Downloads bereitstehen, sind die Listen leer!

Die Ansicht kann beispielsweise wie folgt aussehen:

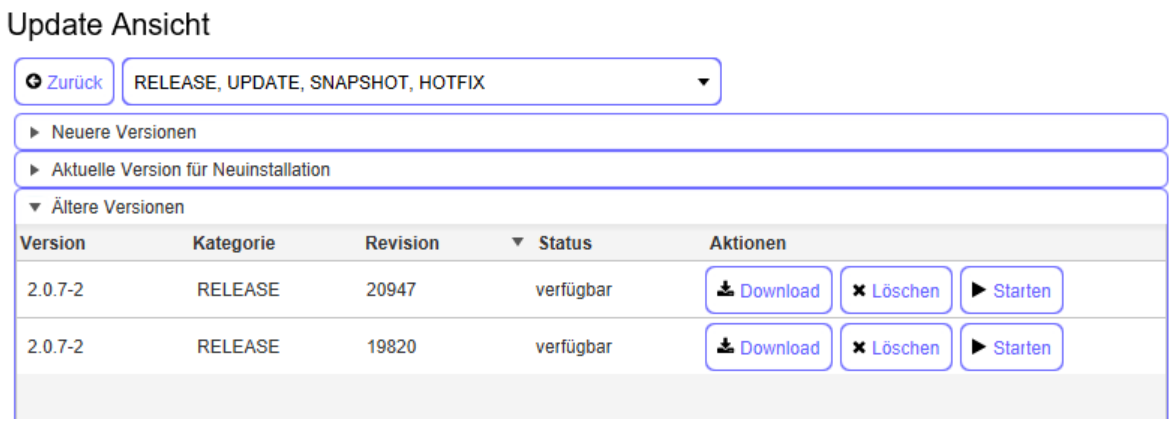

Abbildung 62: KIM-Client – Updates – Beispiel

Sie zeigt, dass zwei ältere Versionen verfügbar sind, und dass es sich dabei um Release-Versionen handelt.

Zum Herunterladen eines Installationspakets drücken Sie den Button „Download“.

Nachdem eine Datei heruntergeladen wurde, wechselt sie vom Status „verfügbar“ in den Status „heruntergeladen“.

Heruntergeladene Dateien können Sie wieder entfernen, indem Sie den Button „Löschen“ drücken. Der Status ändert sich dann wieder auf „verfügbar“.

Sofern Sie heruntergeladene Dateien (Updates) installieren wollen, markieren Sie den entsprechenden Eintrag und drücken dann „Starten“. Die Datei wird ausgeführt.

4.3.3.9.11 Abruf von Zertifikatsinformation einer Telematikkarte (SMC-B od. HBA)

Für den Abruf der Zertifikatsinformationen einer Telematikkarte wählen Sie

- den Konnektor aus, der verwendet werden soll,
- den Mandantenkontext, der im Kontext des Konnektors aufgerufen werden soll und
- die Telematikkarte, dessen Informationen sie abrufen wollen.

Drücken Sie dann neben der Telematikkarte den Button „Zertifikatsdetails“. Es öffnet sich ein Fenster mit den Detailinformationen zur ausgewählten Telematikkarte. Sie haben dort die Möglichkeit, das Zertifikat zu prüfen und im crt-Format zu exportieren.

4.3.3.9.12 Abruf von Zertifikatsinformationen des Client-Modul-Zertifikats

Um die Zertifikatsdetails zum Client-Modul-Zertifikat zu bekommen, gehen Sie folgendermaßen vor:

- Wählen Sie das Menü „Extras“ aus der Menüleiste aus.
- Klicken Sie auf „Zertifikatsdetails“ im Menü.

Es öffnet sich ein Fenster mit den Detailinformationen zum Client-Modul-Zertifikat. Sie haben dort die Möglichkeit, das Zertifikat zu prüfen und im crt-Format zu exportieren.

4.3.4 Abruf von Metriken

Der KIM-Client erfasst Betriebswerte, sog. Metriken. Um die Metriken abzurufen, gehen Sie wie folgt vor:

- Wählen Sie das Menü „Extras“ aus der Menüleiste aus.
- Klicken Sie auf „Metriken“ im Menü.

Es wird ein Fenster angezeigt, dass Ihnen folgende Werte zur Verfügung stellt:

- Gesendete und empfangene E-Mails
- Gesendete und empfangene Bytes für SMTP und POP3
- KAS-Bytes im Up- und Download

Des Weiteren wird Ihnen ein Protokoll der übertragenen Nachrichten als Liste angezeigt:

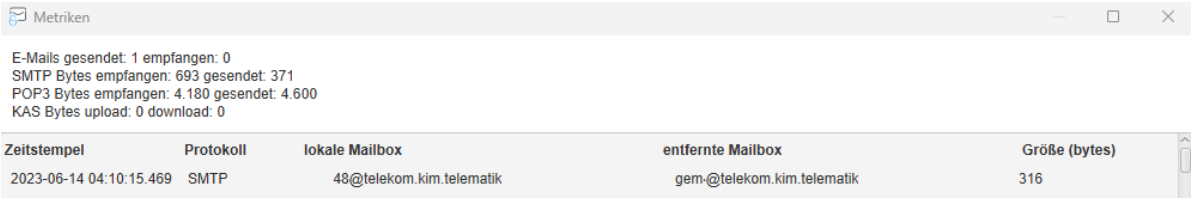

Abbildung 63: KIM-Client - Metriken

Berücksichtigen Sie bitte, dass alle Daten zurückgesetzt werden, sobald der KIM-Client beendet wird. Nach dem Neustart betragen daher alle Werte wieder 0.

Hinweis:

Der Abruf von Metriken ist auch über die JMX-Schnittstelle möglich. Diese ist ausführlich im entsprechenden Schnittstellenhandbuch beschrieben.

4.3.5 Unterstützung und Support

4.3.5.1 E-Mail an KIM-Support senden

Sofern Sie Probleme mit dem Senden bzw. Empfangen von KIM-Nachrichten haben, jedoch den Admin-Client aufrufen können, bietet dieser Ihnen die Möglichkeit, eine E-Mail mittels Ihres Standard-E-Mail-Programms an den KIM-Support zu versenden.

Öffnen Sie dazu im Admin-Client das Menü Unterstützung→E-Mail senden:

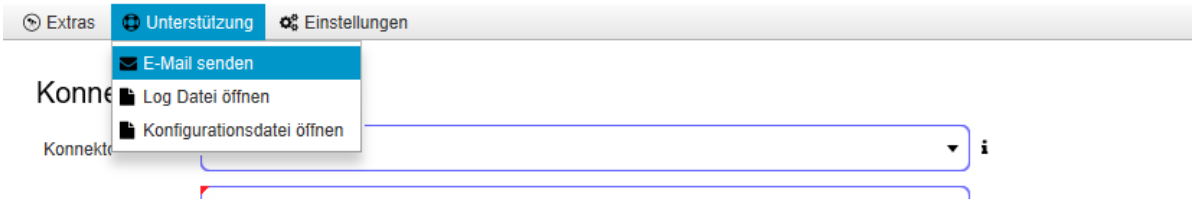

Abbildung 64: KIM-Client – Support-Mail senden

Ihr E-Mail-Programm wir dann ggf. gestartet und eine E-Mail zum Versand vorbereitet. Diese Mail enthält bereits einen einleitenden Satz, den Sie um Details, wie Kundennummer, Fehlerbeschreibung usw. ergänzen.

Senden Sie die so erstellte Nachricht an den KIM-Support.

Diese Funktionalität finden Sie auch in der Account-Ansicht in jeder Zeile unter „…→Unterstützung→E-Mail senden“.

4.3.5.2 Log-Datei öffnen

Sofern Sie Einblick in das Clientmodul-Log benötigen, ist dieses ebenfalls über den Admin-Client möglich.

Rufen Sie dazu folgenden Menüpunkt auf: Unterstützung → Log-Datei öffnen

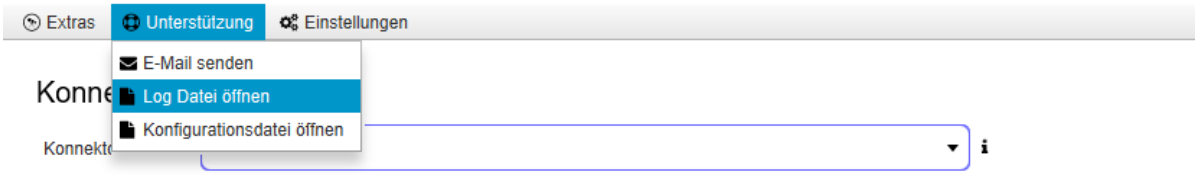

Abbildung 65: KIM-Client – Log-Datei öffnen

Die Log-Datei wird mit Ihrem Standardprogramm für *.log-Dateien geöffnet. Sollte für diese Dateiendung kein Programm registriert sein, schlägt Ihnen das Betriebssystem mögliche Programme vor.

Diese Funktionalität finden Sie auch in der Account-Ansicht in jeder Zeile unter „…→Unterstützung→Log-Datei öffnen“.

4.3.5.3 Konfigurationsdatei öffnen

Sie haben die Möglichkeit, direkt aus dem Admin-Client die Konfigurationsdatei zu öffnen.

Über folgenden Menüeintrag erreichen Sie die Konfigurationsdatei:

Unterstützung → Konfigurationsdatei öffnen

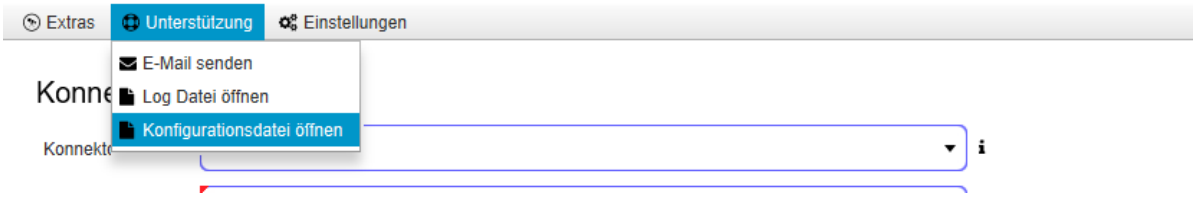

Abbildung 66: KIM-Client – Konfigurationsdatei öffnen

Die Konfigurationsdatei wird mit Ihrem Standardprogramm für *.xml-Dateien geöffnet. Sollte für diese Dateiendung kein Programm registriert sein, schlägt Ihnen das Betriebssystem mögliche Programme vor.

Sofern Sie einen Editor mit der Dateiendung xml verknüpft haben und ggf. Änderungen vornehmen beachten Sie bitte, dass diese erst dann wirksam werden, wenn Sie diese speichern und den KIM-Client neu starten.

Diese Funktionalität finden Sie auch in der Account-Ansicht in jeder Zeile unter „…→Unterstützung→Konfigurationsdatei öffnen“.

4.3.5.4 Support-Dateien hochladen

Ergänzend zu der Unterstützung in der Menüleiste der Anwendung finden Sie in der Account-Ansicht in jeder Zeile unter „…→Unterstützung→Support-Dateien hochladen“ eine komfortable Möglichkeit, dem Support Konfigurations- und Log-Dateien zur Verfügung zu stellen. Für eine Zuordnung der übermittelten Dateien wird die E-Mail-Adresse der betreffenden Zeile mit übertragen.

Folgende Dateien werden an den Support übermittelt:

- Clientmodule.xml
- Clientmodule.log

4.3.5.5 Einstellungen bearbeiten

Ergänzend zum Öffnen der Konfigurationsdatei (wie in Kapitel 4.3.5.3 beschrieben), können Sie die Parameter auch (xml-unabhängig) übersichtlich darstellen und bearbeiten lassen.

Folgen Sie dem Menüeintrag

Einstellungen → Einstellungen anzeigen

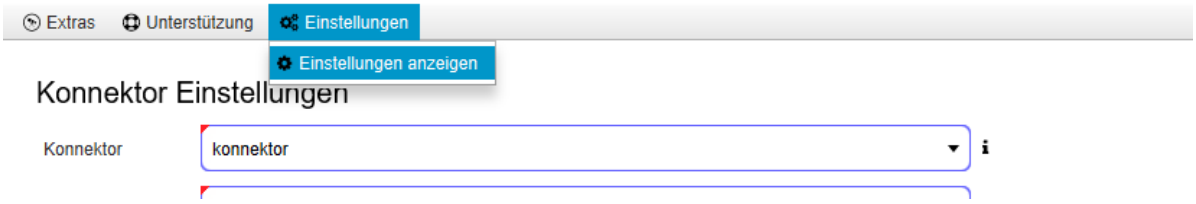

Abbildung 67: KIM-Client – Einstellungen bearbeiten

4.3.6 Abrufen von Versionsinformationen

Um die Versionsinformationen zum KIM-Client abzurufen, gehen Sie wie folgt vor:

- Wählen Sie den KIM-Client aus den Symbolen des Windows-Desktoptrays unten rechts aus. Ggf. ist es erforderlich auch die ausgeblendeten Symbole anzuzeigen.
- Gehen Sie mit dem Mauszeiger über das Symbol des KIM-Clients.
- Drücken Sie die rechte Maustaste.

Wählen Sie „Info“ aus.

Eine andere Möglichkeit zum Abruf der Versionsnummer ist der Aufruf des Admin-Clients. Ist dieser gestartet, können Sie in der Titelleiste der Anwendung die Versionsnummer ablesen.

4.3.7 Nutzung des regelbasierten Kontextmappings (KIMContextRuleMapping)

4.3.7.1 Einführung

Das regelbasierte Kontextmapping ermöglicht Ihnen, während der Verarbeitung einer Mail im KIM-Client, den Aufrufkontext auf Basis von Regeln zu verarbeiten oder zu verändern.

Dabei können sog. Regelblöcke erstellt werden, die wiederum abhängig von der eingesetzten Konnektorstrategie sogar eine Lastverteilung bewirken können.

Der Mechanismus des Kontextmappings ersetzt für alle durch den E-Mail-Ausdruck erfassten E-Mail-Konten diese Angabe durch den des Parameters „context“.

Wichtiger Hinweis:

Das hier vorgestellte regelbasierte Kontextmapping ist sehr umfangreich und erfordert ein tiefgehendes Wissen, wie sich jeder einzelne Parameter auswirkt.

Um Fehler im Vorfeld zu vermeiden, wird dringend angeraten, das komplette Kapitel zum regelbasierten Kontextmapping und die Beispiele durchzulesen und vor Änderung der clientmodule.xml eine Sicherheitskopie zu erstellen.

Bitte bedenken Sie, dass Änderungen an der clientmodule.xml erst nach einem Neustart des KIM-Clients wirksam werden.

4.3.7.2 Default-Mapping

Das Default-Mapping greift dann, wenn keine weitere Regel eingerichtet ist, oder wenn keine andere Regel anwendbar ist.

Das Default-Mapping wird in der clientmodule.xml durch die Knoten

- DefaultSmtpKIMContextRule und
- DefaultPop3KIMContextRule

abgebildet. Das Default-Mapping beinhaltet auch den für den KIM-Client konfigurierten Mandantenkontext. Diese beiden Regeln nutzen eine Default-Domäne. Sie ist abhängig von der

Einsatzumgebung und wird durch das Installationsskript vorgegeben. Sie sollte nicht angepasst werden.

RU-Default-Domäne: „mail-ref.eqxffm.tsi.kim.telematik-test

PU-Default-Domäne: „lb-mail.eqxffm.tsi.kim.telematik

4.3.7.3 Generelle Konfiguration

Zur generellen Konfiguration des regelbasierten Mappings werden zwei Parameter verwendet. Diese sind „enabled“ und „always“.

Wird der Parameter „enabled“ auf „false“ eingestellt, so wird das Rule-Mapping nicht verwendet. Alle konfigurierten Regeln kommen nicht zur Anwendung. Diese greifen erst dann, wenn „enabled“ auf „true“ gesetzt wird.

Vorausgesetzt, dass „enabled“ auf „true“ gesetzt ist, regelt „always“, wann die Regeln zur Anwendung kommen.

Der Default-Wert für „always“ ist „false“. Dies ist die Standardeinstellung. Dadurch wird bewirkt, dass das Rule-Mapping nur dann verwendet wird, wenn der vom E-Mail-Client übermittelte Benutzername keinen Kontext verwendet.

Ist „always“ dagegen „true“, wird das Rule-Mapping immer angewendet, ungeachtet des bereits vom E-Mail-Client im Benutzernamen übermittelten Aufrufkontextes. Ein ggf. mitgelieferter Aufrufkontext wird verworfen und durch den in der Regel konfigurierten ersetzt.

4.3.7.4 Auswahl einer Konnektorstrategie

In der vorliegenden Version des KIM-Clients kommen zwei Konnektorstrategien zum Einsatz:

1. „single“: Diese Strategie wird verwendet, wenn in der Einsatzumgebung des KIM-Clients nur ein Konnektor Anwendung finden soll. Beachten Sie, dass Sie auch „single“ konfigurieren können, wenn sich in der Einsatzumgebung mehrere Konnektoren befinden, jedoch nur einer verwendet werden soll.
2. „roundrobbin“: Verwenden Sie „roundrobbin“, wenn Sie mindestens zwei Konnektoren für das regelbasierte Kontextmapping verwenden möchten.

Hinweis:

Bitte beachten Sie, dass Sie für die Strategie „roundrobbin“ die verwendeten Konnektoren entsprechend identisch konfigurieren müssen, so dass die Kontexte auf allen am roundrobbin-Verfahren teilnehmenden Konnektoren gleich sind. Des Weiteren müssen Sie darauf achten, dass für die Aufrufkontexte Zwillingskarten eingesetzt werden. Diese Karten besitzen zwar unterschiedliches Schlüsselmaterial, verwenden jedoch dieselbe Telematik-ID.

4.3.7.5 Erstellen und Verwenden von Regeln

Regeln werden in der Datei clientmodule.xml erstellt. Grundsätzlich ist für jede Regel ein eigener Eintrag zu erstellen. Die Regeln werden im Abschnitt „KIMContextRuleMapping“ eingetragen. Eine Beschreibung der Parameter einer Regel finden Sie im Kapitel 4.6.8.1.

4.3.7.6 Einsatz von Wildcards

Es können folgende Wildcards verwendet werden:

„&“ ersetzt genau ein Zeichen an der dedizierten Position.

„*“ ersetzt eine beliebige Anzahl von Zeichen an der dedizierten Position. Dieses Zeichen darf nicht eingebettet werden und kann nur einmal pro Ausdruck verwendet werden. Beispiel zum Einsatz von Wildcards finden sich im Kapitel 4.3.7.7.3ff.

4.3.7.7 Beispiele

4.3.7.7.1 Anhängen eines festen Mandantenkontextes an einen Benutzernamen

Sowohl in einer Ein-Konnektor- als auch einer Multi-Konnektor-Umgebung kann es sinnvoll sein, einen festen Mandantenkontext zu verwenden. Dies ist z.B. dann erforderlich, wenn der E-Mail-Client keine komplexen Benutzernamen (z.B. die Hash-Tags #) unterstützt.

Für die Erstellung einer Regel benötigen Sie folgende Informationen:

Parameter	Beispieldaten
E-Mail-Adresse	info@meine-arztpraxis.kim.telematik
Kontext	M0, C0, A0
Id	Praxisregel_SMTP
Port	465

Tabelle 4: Informationen für die Erstellung einer Regel

Diese Bestandteile formatieren Sie folgendermaßen:

context=“meine-arztpraxis.kim.telematik:465#M0#C0#A0“

id=“Praxisregel_SMTP“

protocol=“smtp“

Die formatierten Bestandteile fügen Sie nun zu einer Regel zusammen:

<KIMContextRule context=“meine-arztpraxis.kim.telematik:465#M0#C0#A0“ id=“Praxisregel_SMTP“ protocol=“smtp“**>**info@meine-arztpraxis.kim.telematik**</KIMContextRule>**

Zur Erstellung eines einfachen Regelsatzes sollte auch für POP3 eine entsprechende Regel verwendet werden.

Unter der Annahme, dass für POP3 der Port 995 verwendet wird, ergibt sich dann folgende Regel:

<KIMContextRule context=“meine-arztpraxis.kim.telematik:995#M0#C0#A0“ id=“Praxisregel_POP3“ protocol=“pop3“**>**info@meine-arztpraxis.kim.telematik**</KIMContextRule>**

4.3.7.7.2 Regel für alle Mail-Adressen einer Domäne erstellen

Dieser Ansatz bietet sich insbesondere dann an, wenn Sie eine eigene E-Mail-Domäne besitzen und alle KIM-E-Mail-Adressen einem Mandantenkontext zugeordnet haben.

Angenommen, Sie besäßen die Domäne „meine-institution.kim.telematik“.

Um für alle Mail-Adressen dieser Domäne eine Regel zu erstellen, machen Sie Gebrauch vom Wildcard „*“ und ersetzen hiermit den Local-Part der E-Mail-Adresse.

Der Parameter E-Mail-Adresse sähe dann so aus: „*@meine-institution.kim.telematik“.

Hieraus ergibt sich dann folgender Regeleintrag in der clientmodule.xml:

<KIMContextRule context=“meine-institution.kim.telematik:995#M0#C0#A0“ id=“Praxisregel_POP3“ protocol=“pop3“**>***@meine-institution.kim.telematik**</KIMContextRule>**

Diese Regel können Sie aber auch auf die Default-Domänen anwenden, sofern Sie über keine eigene Domäne verfügen.

In der PU und für die T-Systems-Domäne ergäbe sich dann z.B.:

<KIMContextRule context=“lb-mail.eqxffm.tsi.kim.telematik:995#M0#C0#A0“ id=“Praxisregel_POP3“ protocol=“pop3“**>***@tsi.kim.telematik**</KIMContextRule>**

Für die PU und die Default-Domäne der Telekom sähe die Regel folgendermaßen aus:

<KIMContextRule context=“lb-mail.eqxffm.telekom.kim.telematik:995#M0#C0#A0“ id=“Praxisregel_POP3“ protocol=“pop3“**>***@telekom.kim.telematik**</KIMContextRule>**

4.3.7.7.3 Einsatz von Wildcards im lokalen Teil von E-Mail-Adressen

Hinweis: Es ist nur ein Wildcard im lokalen Teil erlaubt.

<u>Beispiel 1: nur „*“:</u>

<KIMContextRule context=“lb-mail.eqxffm.telekom.kim.telematik:995#M0#C0#A0“ id=“Praxisregel_POP3“ protocol=“pop3“**>***@telekom.kim.telematik**</KIMContextRule>**

Ergebnis:

Alle über diese Domäne verfügenden Mail-Adressen werden mit dem konfigurierten Kontext umgesetzt.

<u>Beispiel 2: „*“ am Ende des lokalen Teils:</u>

<KIMContextRule context=“lb-mail.eqxffm.telekom.kim.telematik:995#M0#C0#A0“ id=“Praxisregel_POP3“ protocol=“pop3“**>**info*@telekom.kim.telematik**</KIMContextRule>**

Ergebnis:

Alle konfigurierten Mail-Adressen, die mit „info“ beginnen und im lokalen Teil weitere folgende Zeichen enthalten, werden mit dem konfigurierten Kontext umgesetzt. Dies erfolgt z.B. für „info1“, „info2“ usw. aber auch für „info27“ oder „info_Labor“.

Beispiel 3: „?“ am Ende des lokalen Teils:

<KIMContextRule context=“lb-mail.eqxffm.telekom.kim.telematik:995#M0#C0#A0“ id=“Praxisregel_POP3“ protocol=“pop3“**>**info?@telekom.kim.telematik**</KIMContextRule>**

Ergebnis:

Alle konfigurierten Mail-Adressen, die mit „info“ beginnen und im lokalen Teil genau ein weiteres Zeichen enthalten werden mit dem konfigurierten Kontext umgesetzt. Dies erfolgt z.B. für „info1“, „info2“ usw. in der Domäne „telekom.kim.telematik“. „info11“ entspricht nicht der Regel, da hierfür „…info1?@...“ anzugeben wäre.

4.3.7.7.4 Einsatz von Wildcards im Domänenteil von E-Mail-Adressen

Hinweise: Es ist nur ein Wildcard im Domänenteil erlaubt. Der Einsatz von Wildcards im Domänenteil ist dann sinnvoll, wenn mehrere eigene Domänen adressiert werden sollen.

Beispiel 1: „*“ am Anfang des Domänenteils:

<KIMContextRule context=“lb-mail.eqxffm.telekom.kim.telematik:995#M0#C0#A0“ id=“Praxisregel_POP3“ protocol=“pop3“**>**info@*.kim.telematik**</KIMContextRule>**

Ergebnis:

Es werden mehrere Domänen, z.B. „kh_verbund_ost.kim.telematik“ und „kh_verbund_west.kim.telematik“ über diese Regel adressiert. Bitte beachten Sie, dass dabei der Mandantenkontext sowie das zu adressierende Kartenmaterial (SMC-B) domänenübergreifend zur Verfügung stehen muss.

Beispiel 2: „?“ im Domänenteil:

<KIMContextRule context=“kh_oderritz.kim.telematik:995#M0#C0#A0“ id=“KH_Regel_POP3“ protocol=“pop3“**>***@station?.kh_oderritz.kim.telematik**</KIMContextRule>**

Ergebnis:

Es werden mehrere Domänen, z.B. „station1.kh_oderritz.kim.telematik“ und „station2.kh_oderritz.kim.telematik“ über diese Regel adressiert. „station27.kh_oderritz.kim.telematik“ würde nicht adressiert werden, da „?“ lediglich ein Zeichen ersetzt.

4.3.7.7.5 Beispiel einer komplexen Konnektorstrategie

Eine komplexe Konnektorstrategie kann mit mehreren Regelsätzen umgesetzt werden.

Regelsätze werden durch den Knoten <KIMContextRules> gekapselt.

Beispiel: KH mit drei Konnektoren, davon ein Konnektor Stand-Alone und einer Domäne und zwei weitere im Load-Balancing und zwei weiteren Domänen:

Lösung: Es werden zwei Rulesets benötigt:

Ruleset 1 mit type="single" mit einem Konnektor und einer Domäne

<KIMContextRule context=" apo.kh_oderritz.kim.telematik:995#M0#C0#A0" id="KH_Regel_POP3" protocol="pop3"**>***@apo.kh_oderritz.kim.telematik**</KIMContextRule>**

Ruleset 2 mit type="roundrobbin" mit zwei Konnektoren und zwei weiteren Domänen

<KIMContextRule context="station.kh_oderritz.kim.telematik:995#M0#C0#A0" id="KH_Regel_POP3" protocol="pop3"**>***@station?.kh_oderritz.kim.telematik**</KIMContextRule>**

Bitte beachten Sie, dass diese Konstellation folgende Eigenschaften hat:

- Es werden alle Adressen der Domäne „apo.kh_oderritz.kim.telematik" durch Ruleset 1 verarbeitet. Es wird dafür ein Konnektor genutzt.
- Es werden alle Adressen der Domänen „station1…" bis „station9…" des kh_oderritz durch Ruleset 2 verarbeitet. Es werden zwei Konnektoren via „roundrobbin" verwendet.
  Die Mail-Adressen müssen stationsübergreifend eindeutig sein:
  - „info@station1" und „info@station2" ist hier nicht möglich!
  - „info_prim@station1" und „info_sek@station2" sind möglich!
- Die Mandantenkontexte müssen auf beiden Konnektoren angelegt sein.
- Es müssen Zwillingskarten mit derselben Telematik-ID verwendet werden.

4.4 Technische Anwendungsfälle

4.4.1 Konfiguration einer Multikonnektor-Umgebung

Zur Konfiguration einer Multikonnektor-Umgebung gehen Sie wie folgt vor.

- Installieren Sie den KIM-Client wie gewohnt. Dabei konfigurieren Sie bereits den ersten Konnektor.
- Öffnen Sie die Konfigurationsdatei clientmodule.xml. Sie finden diese Datei im Unterverzeichnis conf Ihrer KIM-Client-Installation.
- Kopieren Sie den kompletten Knoten <connector … /connektor> direkt unter den bestehenden connector-Knoten.
- Passen Sie die Parameter zum zweiten Knoten von Hand an (Url, Zugangsdaten, Aufrufkontext, Authentisierung usw.). Erläuterungen zu den Parametern finden Sie im Kapitel 4.6.7.
- Speichern Sie Ihre Änderungen.

4.4.2 Umstellung des JMX-Ports (RMI)

In bestimmten Primärsystemumgebungen kann es vorkommen, dass der JMX-Port des KIM-Clients bereits durch eine andere Anwendung genutzt wird. In diesem Fall startet der KIM-Client nicht.

Sie können die Konfiguration des KIM-Clients jedoch schnell selbst ändern:

- Öffnen Sie die Konfigurationsdatei clientmodule.xml. Sie finden diese Datei im Unterverzeichnis conf Ihrer KIM-Client-Installation.
- Suchen Sie den Knoten Configuration→ClientModule→JMX→rmiRegistryPort
- Ändern Sie die Portnummer auf einen beliebigen freien Port.
- Speichern Sie Ihre Änderungen.

Testen Sie die Konfiguration, indem Sie die Anwendung starten.

4.4.3 Verwendung des KIM-Security-Interfaces

4.4.3.1 Einführung

Das KIM-Security-Interface ist eine optionale Komponente, die es Ihnen ermöglicht, vor der Zustellung einer Mail an den Mail-Client diese durch einen Virenscanner prüfen zu lassen.

Diese Komponente verfügt über eine eigene Installation und ist damit nicht Bestandteil des KIM-Clients. Zu Installation und Konfiguration des Interfaces greifen Sie bitte auf die entsprechende Dokumentation zurück.

Im Nachfolgenden wird lediglich die Anbindung des KIM-Clients an ein bereits konfiguriertes Interface dargestellt.

4.4.3.2 Gegenüberstellung Virenscanner-Schnittstelle vs. KIM-Security-Interface

Genauso, wie das KIM-Security-Interface, ermöglicht auch die im Kapitel 4.4.4 beschriebene Virenscanner-Schnittstelle es Ihnen, einen Virenscanner einzubinden. Beide Mechanismen sprechen jedoch unterschiedliche Nutzergruppen an.

Mittels Virenscanner-Schnittstelle kann jeder über das Windows-Betriebssystem verfügbare Virenscanner via AMSI eingebunden werden. Im Gegensatz zum KIM-Security-Interface besitzt diese Schnittstelle jedoch keinen Mailcache, so dass die E-Mails dort synchron während des Abholens überprüft werden. Diese Schnittstelle ist somit eher für kleinere bis mittelgroße Einrichtungen geeignet.

Sofern der KIM-Client jedoch in einer größeren Einrichtung betrieben werden soll, empfiehlt es sich, stattdessen das KIM-Security-Interface zu nutzen. Dieses speichert alle vom Fachdienst abgeholten Nachrichten zunächst zwischen und leitet diese selbständig an den Virenscanner weiter. Der einzubindende Virenscanner muss SMTP-Forwarding für die Weiterleitung geprüfter Mails an den Mailcache beherrschen. Der Mailclient holt die Mails dann nicht mehr vom KIM-Client ab, sondern vom Mailcache des KIM-Security-Interfaces. Dieser Ansatz wird vornehmlich von großen bis sehr großen Einrichtungen genutzt.

4.4.3.3 Voraussetzungen

Grundsätzliche Voraussetzung für die Verwendung des KIM-Security-Interfaces mit dem KIM-Client ist dessen Installation und Verfügbarkeit.

Eine spätere Konfiguration des KIM-Clients ist jedoch ebenfalls möglich und in Kapitel 4.4.3.5 beschrieben.

Die Voraussetzungen für das Security-Interface sind in der entsprechenden Dokumentation nachzulesen.

Wichtiger Hinweis: Bitte beachten Sie, dass die Integration des KIM-Security-Interfaces im Normalfall auch Anpassungen an betroffenen Benutzerkonten nach sich ziehen.

4.4.3.4 Konfiguration während des Installationsprozesses

Die Konfiguration des KIM-Clients zur Nutzung des Mailcaches ist im Kapitel 3.3.3 beschrieben.

4.4.3.5 Nachträgliche Konfiguration einer bestehenden Installation

Hinweis: Es wird empfohlen, eine Konfiguration während des Installationsprozesses durchzuführen. Näheres hierzu erfahren Sie im vorstehenden Kapitel.

Sofern Sie einen Mailcache in eine bestehende KIM-Client-Installation einbinden wollen, müssen Sie Anpassungen an der clientmodule.xml vornehmen.

Gehen Sie dafür wie folgt vor:

1. Beenden Sie den KIM-Client.
2. Öffnen Sie mit einem Editor (z.B. Notepad++) die Datei clientmodule.xml. Sie finden diese Datei im Unterverzeichnis /conf des Installationsverzeichnis.
3. Navigieren Sie im Editor in den Knoten „Mailcache“.
4. Setzten Sie dort den Parameter „enabled“ auf „true“.
5. Geben Sie unter „Url“ die Url an, unter der der Mailcache erreichbar ist, z.B. http://localhost:8001.
6. Prüfen Sie die Default-E-Mail-Domain. Insbesondere wenn Sie über eine eigene Domäne verfügen, sollten Sie den Eintrag entsprechend anpassen.
7. Speichern Sie die Datei, und schließen Sie den Editor.
8. Starten Sie den KIM-Client neu.

Damit ist die manuelle Konfiguration abgeschlossen.

4.4.4 Konfiguration der Virenscanner-Schnittstelle

4.4.4.1 Einführung

Die aktuelle Version des KIM-Clients ermöglicht es Ihnen, einen lokalen Virenscanner – auch ohne die Nutzung des KIM-Security-Interfaces einzubinden.

Zum einen bietet der KIM-Client dafür die Integration der AMSI-Schnittstelle des Windows-Betriebssystems an, zum anderen kann der Virenscanner ClamAV eingebunden werden.

Hinweis:

Die Konfiguration zur Nutzung der AMSI-Schnittstelle während des Installationsprozesses ist in Kapitel 3.3.3 beschrieben.

Eine Anbindung an ClamAV während des Installationsprozesses ist nicht möglich. Gehen Sie in diesem Fall gem. Kapitel 4.4.4.3 vor.

4.4.4.2 Einbindung der AMSI-Schnittstelle

Um die AMSI-Schnittstelle nutzen zu können, gehen Sie folgendermaßen vor:

1. Beenden Sie den KIM-Client.
2. Öffnen Sie mit einem Editor (z.B. Notepad++) die Datei clientmodule.xml. Sie finden diese Datei im Unterverzeichnis /conf des Installationsverzeichnis.
3. Navigieren Sie im Editor in den Knoten „AntiVirusEngines“.
4. Setzten Sie dort den Parameter „activeEngine“ auf „AMSI“.
5. Setzen Sie den Parameter „enabled“ auf „true“.
6. Setzen Sie die Parameter „pop3“ und „smtp“ auf „true“.
7. Speichern Sie die Datei, und schließen Sie den Editor.
8. Starten Sie den KIM-Client neu.

Damit ist die manuelle Konfiguration abgeschlossen.

4.4.4.3 Einbindung von ClamAV

Wichtiger Hinweis:

Stellen Sie sicher, dass Sie den ClamAV-Virenscanner installiert und konfiguriert haben. Stellen Sie weiterhin sicher, dass der KIM-Client den Virenscanner erreichen kann.

Für die Einbindung des ClamAV-Virenscanners, gehen Sie folgendermaßen vor:

1. Beenden Sie den KIM-Client.
2. Öffnen Sie mit einem Editor (z.B. Notepad++) die Datei clientmodule.xml. Sie finden diese Datei im Unterverzeichnis /conf des Installationsverzeichnis.
3. Navigieren Sie im Editor in den Knoten „AntiVirusEngines“.
4. Setzten Sie dort den Parameter „activeEngine“ auf „ClamAVTCPClient“.

5. Setzen Sie den Parameter „enabled“ auf „true“.
6. Setzen Sie die Parameter „pop3“ und „smtp“ auf „true“.
7. Setzen Sie den Knoten „ClamAVTCPClient→Hostname“ auf den Hostname, auf dem Sie ClamAV installiert haben. Sofern Sie ClamAV auf demselben Rechner installiert haben, wie den KIM-Client, tragen Sie „localhost“ ein.
8. Setzen Sie den Knoten „ClamAVTCPClient→Port“ auf den von Ihnen konfigurierten Port von ClamAV. Der Standardport ist „3310“.
9. Konfigurieren Sie bei Bedarf die Parameter ClamAVTCPClient→ConnectTimeout und ClamAVTCPClient→ReadTimeout. Beide Parameter sind mit Default-Werten von jeweils 10 Sekunden vorbelegt.
10. Speichern Sie die Datei, und schließen Sie den Editor.
11. Starten Sie den KIM-Client neu.

Damit ist die manuelle Konfiguration abgeschlossen.

4.4.4.4 Verwendung der ICAP-Schnittstelle

Die Verwendung der ICAP-Schnittstelle ist durch eine manuelle Konfiguration der clientmodule.xml möglich. Bitte berücksichtigen Sie, dass ggf. weitere Einstellungen an Ihrem ICAP-Server vorgenommen werden müssen.

Gehen Sie für die Konfiguration folgendermaßen vor:

1. Beenden Sie den KIM-Client.
2. Öffnen Sie mit einem Editor (z.B. Notepad++) die Datei clientmodule.xml. Sie finden diese Datei im Unterverzeichnis /conf des Installationsverzeichnis.
3. Navigieren Sie im Editor in den Knoten „AntiVirusEngines“.
4. Setzten Sie dort den Parameter „activeEngine“ auf „ICAP“.
5. Setzen Sie den Parameter „enabled“ auf „true“.
6. Setzen Sie die Parameter „pop3“ und „smtp“ auf „true“.
7. Setzen Sie den Knoten „ICAPClient→Hostname“ auf den Hostname, auf dem Sie den ICAP-Server installiert haben. Sofern Sie den anzubindenden Server auf demselben Rechner installiert haben, wie den KIM-Client, tragen Sie „localhost“ ein.
8. Setzen Sie den Knoten „ICAPClient→Port“ auf den von Ihnen konfigurierten Port des ICAP-Servers. Der Standardport ist „1344“.
9. Vergeben Sie bei Bedarf einen Dienstenamen im Parameter ICAPClient→Servicename. Standardmäßig ist dieser Wert mit „virus_scan“ bereits konfiguriert.
10. Konfigurieren Sie die TLS-Verbindungssicherheit mit ICAPClient→Secure. Standardmäßig ist dieser Wert auf „false“ gesetzt.
11. Konfigurieren Sie bei Bedarf die Parameter ICAPClient→ConnectTimeout und ICAPClient→ReadTimeout. Beide Parameter sind mit Default-Werten von jeweils 10 Sekunden vorbelegt.

12. Speichern Sie die Datei, und schließen Sie den Editor.
13. Starten Sie den KIM-Client neu.

Damit ist die manuelle Konfiguration abgeschlossen.

4.5 Sonstige Anwendungsfälle

4.5.1 Kennwort zum E-Mail-Konto vergessen

Bitte wenden Sie sich in diesem Fall an Ihren Support. Öffnen Sie ein Ticket zur Kennwort-Rücksetzung.

4.6 Technische Konfiguration

Dieses Kapitel stellt die Aufgaben vor, dies sich aus dem Betrieb des KIM-Clients ergeben. Diese Beschreibung ist für alle Betriebssystemkonfigurationen grundsätzlich gleich. Daher wird an dieser Stelle die Windows-Implementierung stellvertretend für alle anderen unterstützten Konfigurationen dargestellt.

Die Standardkonfiguration des KIM-Clients ist im Allgemeinen für die meisten Anwendungsfälle ausreichend.

Bei Bedarf kann die Konfiguration des KIM-Clients jedoch angepasst werden.

Wichtiger Hinweis: Eventuelle Anpassungen an der Konfiguration des KIM-Clients werden ggf. erst nach einem Neustart des Clients wirksam.

Nachfolgend werden Ihnen die Parameter und ihre Funktion beschrieben.

4.6.1 Speicherort der Konfigurationsdatei

Die Konfigurationsdatei des KIM-Clients finden Sie im Installationsverzeichnisses des Clients. Die Bezeichnung lautet clientmodule.xml.

4.6.2 Aufbau der Konfigurationsdatei

Die Konfigurationsdatei gliedert sich in verschiedene Abschnitte. Diese sind

Abschnittsbezeichnung	Beschreibung
ClientModule	Beschreibt das eigene Verhalten
WebPortalRest	Definiert die REST-Schnittstelle zum Webportal
ClientSystem	Definiert das Verhalten ggü. einem E-Mail-Client
MailTransferAgent	Definiert das Verhalten ggü. dem Fachdienst KIM
Connectors	Definiert das Verhalten ggü. Konnektoren
KIMContextRuleMapping	Definiert anzuwendende Regeln in Abhängigkeit vom Aufrufkontext
AdminClient	Definiert das Verhalten des Administrationsclients
RestAPI	Definiert die REST-Schnittstelle zum Fachdienst
MailCache	Definiert die Nutzung eines lokalen Mailcaches
AntiVirusEngines	Definiert die Anbindung an eine lokale Virenscanner-Lösung ohne Mailcache

Tabelle 5: Abschnitte der Konfigurationsdatei Clientmodule.xml

4.6.3 Parameterliste Clientmodule

Name	Default-Wert	Beschreibung
JMX	-	Siehe Kapitel 4.6.3.1.
MaxMailSize	734003200	Legt die maximal durch den KIM-Client zu verarbeitende Größe einer Nachricht einschl. Anhangs fest.
MaxThreads	5	Legt die Anzahl der maximal durch das Clientmodul verarbeitbaren Anfragen (Mailversand/Mailempfang) fest.
MaxRestThreads	5	Legt die Anzahl der maximal durch das Clientmodul verarbeitbaren REST-Anfragen fest.
DisabledFeatures	-	Ermöglich das Ausschalten bestimmter Verarbeitungsschritte. Dieser Parameter ist im Wirkbetrieb leer!
TTLEncCert	12 hours	Caching-Dauer für Verschlüsselungszertifikate.
TTLEmailIccsn	30 days	Caching-Dauer für das Speichern der Zuordnung von E-Mail-Adressen zu ICCSN.
TTLCertStatus	24 hours	Caching-Dauer für TLS-Zertifikate.
InteractiveMode	Für Client: true Für Dämon: false	Legt fest, ob Informationen zum Verarbeitungsstand von Nachrichten angezeigt werden, oder nicht.
TempFileLocation	-	Nur zur internen Verwendung
QuartzJobScheduler	Priority="5" Threads="3"	Interner Job-Zeitplanungsassistent
DefaultEMailDomain	TU/RU: telekom.kim.telematik-test PU: telekom.kim.telematik	Default-Domäne

Name	Default-Wert	Beschreibung
DefaultEMailServer	RU: mail-ref.eqxffm.tsi.kim.te-lematik-test PU: lb-mail.eqxffm.tsi.kim.te-lematik	Fachdienstname, unter dem der E-Mail-Dienst zu erreichen ist.
DNS-SD	-	Siehe Kapitel 4.6.3.2.

Tabelle 6: Parameterliste Clientmodule

4.6.3.1 Unterparameter JMX

Name	Default-Wert	Beschreibung
Username	-	Benutzername für Remote-JMX-Verbindungen
Password	-	Kennwort zum Benutzernamen
rmiRegistryPort	9100	Standardport, auf dem JMX registriert wird
rmiServer	0.0.0.0:9101	Port, auf dem der RMI-Server bereitgestellt wird
useCustomSSLClientSocketFactory	True	Ermöglichen von Remote-Aufrufen via TLS: True = Remote-Aufrufe via TLS False = Keine Remote-Aufrufe via TLS
Connection	-	Siehe Kapitel 4.6.3.1.1

Tabelle 7: Clientmodule – JMX

4.6.3.1.1 Unterparameter Connection

Name	Default-Wert	Beschreibung
AuthMode	NONE	Bestimmt die Authentifizierungsmethode (NONE od. SRV)
SSLEnabled-Protocols	TLSv1.2	Legt den zugrunde liegenden TLS-Standard für die Verschlüsselung fest.
CipherSuites	Siehe Anhang A.4 „Liste verwendeter Cipher-Suiten”	Durch den KIM-Client unterstützte Ciphersuites an dieser Schnittstelle.
Keystore	Type = „PKCS12“ <absoluter Pfad >\clientmodule_key-store.p12	Legt die Bezeichnung des verwendeten Schlüsselspeichers fest. Der Parameter „type“ muss dem Keystore-Typen entsprechen (hier also „PKCS12“).
KeystorePass-word	ENC(…)	Beinhaltet das Kennwort zum Schlüsselspeicher.
KeyAlias	<Rechnername>	Beinhaltet einen Alias-Namen für den Schlüssel des Clientmoduls.
KeyPassword	ENC(…)	Beinhaltet das Kennwort zum Schlüssel.
Truststore	Type=“PKCS12“ clientsystem_truststore.p12	Legt die Bezeichnung des verwendeten Zertifikatsspeichers fest. Der Parameter „type“ muss dem Truststore-Typen entsprechen.
Truststore-Password	ENC(...)	Beinhaltet das Kennwort zum Zertifikatsspeicher.

Tabelle 8: Parameterliste JMX - Connection

4.6.3.2 Unterparameter DNS-SD

Name	Default-Wert	Beschreibung
Domain	TU/RU: kim.telematik-test PU: kim.telematik	Domänenname der Service-Records
Enabled	True	Wenn true, dann Nutzen des DNS-Service Discovery, ansonsten false
Server	<IP-Adresse>	IP-Adresse, unter der der DNS-Server erreichbar ist.
KASServiceType	_kas._tcp.	KAS-Service-Typ-Bezeichnung
SmtpServiceType	_fdkimsmtp._tcp.	SMTP-Service-Typ-Bezeichnung
Pop3ServiceType	_fdkimpop._tcp.	POP3-Service-Typ-Bezeichnung
WPServiceType	_accmgr._tcp.	Web-Portal-Service-Typ-Bezeichnung

Tabelle 9: Clientmodule – DNS-SD

4.6.4 Parameterliste WebPortalRest

Name	Default-Wert	Beschreibung
Enabled	True	Nutzung der Web-Portal-REST-Schnittstelle
useDNS	True	Verwendung der DNS-Namensauflösung für diese Schnittstelle
Url	-	Legt den Aufruflink zur REST-Schnittstelle des Webportals fest.
Connection	-	Siehe Kapitel 4.6.4.1.

Tabelle 10: Parameterliste WebPortalRest

4.6.4.1 Unterparameter Connection

Name	Default-Wert	Beschreibung
UseOpenssl-Provider	false	Keine
Proxy	Enabled = “false” http = “true” password = “” user = “”	Bestimmt die Proxy-Einstellungen
ConnectionTimeout	10 Sekunden	Legt fest, nach welcher Zeit die Verbindung geschlossen wird.
ReadTimeout	30 Sekunden	Legt fest, nach welcher Wartezeit in der Operation Read die Verbindung geschlossen wird.
AuthMode	SRV	Bestimmt die Authentifizierungsmethode (NONE od. SRV)
SSLEnabled-Protocols	TLSv1.2	Legt den zugrunde liegenden TLS-Standard für die Verschlüsselung fest.
CipherSuites	Siehe Anhang A.4 „Liste verwendeter Cipher-Suiten”	Durch den KIM-Client unterstützte Ciphersuites in Richtung Webportal-REST-API
DisableCN-Check	true	Ermöglicht, die Überprüfung des Hostnamens (common name) abzuschalten.

Name	Default-Wert	Beschreibung
Truststore	Type=“PKCS12“ webportal_truststore.p12	Legt die Bezeichnung des verwendeten Zertifikatsspeichers fest. Der Parameter „type“ muss dem Truststore-Typen entsprechen.
Truststore-Password	ENC(...)	Beinhaltet das Kennwort zum Zertifikatsspeicher.

Tabelle 11: Parameterliste WebPortalRest - Connection

4.6.5 Parameterliste ClientSystem

Name	Default-Wert	Beschreibung
Enabled	True	Verwendung eines Clientsystems
SmtpHostname	0.0.0.0	Ermöglicht die Bindung durch jeden Client im Netzwerk.
SmtpPort	465	Lokaler Port, auf dem ein E-Mail-Client Nachrichten an den Fachdienst übermitteln kann.
Pop3Hostname	0.0.0.0	Ermöglicht die Bindung durch jeden Client im Netzwerk.
Pop3Port	995	Lokaler Port, auf dem ein E-Mail-Client Nachrichten vom Fachdienst abholen kann.
SmtpTimeout	5 min	Zeitspanne, für die die clientseitige SMTP-Verbindung kommandolos aufrechterhalten wird.
Pop3Timeout	5 min	Zeitspanne, für die die clientseitige POP3-Verbindung kommandolos aufrechterhalten wird.
Connection	-	Siehe Kapitel 4.6.5.1

Tabelle 12: Parameterliste ClientSystem

4.6.5.1 Unterparameter Connection

Name	Default-Wert	Beschreibung
AuthMode	-	Definiert die Authentisierungsmethode zum Clientsystem. Mögliche Werte: NONE, SRV, C_X509
SSLEnabled-Protocols	TLSv1.2	Legt die möglichen Versionen des Verschlüsselungsprotokolls zum E-Mail-Client fest.
CipherSuites	Siehe Anhang A.4 „Liste verwendeter Cipher-Suiten”	Durch das Clientmodul unterstützte Ciphersuites in Richtung Clientsystem.
Keystore	Type = „PKCS12“ <absoluter Pfad >\clientmodule_keystore.p12	Legt die Bezeichnung des verwendeten Schlüsselspeichers fest. Der Parameter „type“ muss dem Keystore-Typen entsprechen (hier also „PKCS12“).
Keystore-Password	ENC(…)	Beinhaltet das Kennwort zum Schlüsselspeicher.
KeyAlias	<Rechnername>	Beinhaltet einen Alias-Namen für den Schlüssel des Clientmoduls.
KeyPassword	ENC(…)	Beinhaltet das Kennwort zum Schlüssel.
Truststore	Type=“PKCS12“ Clientsystem_truststore.p12	Legt die Bezeichnung des verwendeten Zertifikatsspeichers fest. Der Parameter „type“ muss dem Truststore-Typen entsprechen.
Truststore-Password	ENC(…)	Beinhaltet das Kennwort zum Zertifikatsspeicher, sofern konfiguriert.

Tabelle 13: Parameterliste ClientSystem/Connection

4.6.6 Parameterliste MailTransferAgent

Name	Default-Wert	Beschreibung
Enabled	True	Nutzung des MTA
useDNS	True	Namensauflösung via DNS
SmtpTimeout	5 min	Zeitspanne, für die die serverseitige SMTP-Verbindung zum Fachdienst kommandolos aufrechterhalten wird.
Pop3Timeout	5 min	Zeitspanne, für die die serverseitige POP3-Verbindung kommandolos aufrechterhalten wird.
KIMAttachmentService	-	Siehe Kapitel 4.6.6.1
Connection	-	Siehe Kapitel 4.6.6.2

Tabelle 14: Parameterliste MailTransferAgent

4.6.6.1 Unterparameter KIMAttachmentService

Name	Default-Wert	Beschreibung
URL	Umgebungs-abhängig	URL zum Fachdienst KIM
Threshold	15728640	Größe der Mail ab der der KIM-Attachments-ervice genutzt wird (entspricht 15 MiB).
ExpiresAfter	90 Tage	Dauer, nach der der Anhang gelöscht wird.
ConnectTimeout	10 Sekunden	Zeitspanne, für die die Verbindung ohne Transfer aufrechterhalten wird.
ReadTimeout	30 Sekunden	Zeitspanne, für die die Verbindung zum Le-sen aufrechterhalten wird.

Tabelle 15: Parameterliste MailTransferAgent – KIMAttachmentService

4.6.6.2 Unterparameter Connection

Name	Default-Wert	Beschreibung
UseOpensslProvider	False	True, wenn OpenSSL als Security-Provider genutzt wird, ansonsten false.
Proxy	Enabled="false" http="true" password="" socks="false" user=""	Legt die Proxy-Funktionalität für den MTA fest.
ConnectTimeout	10 Sekunden	Legt die Wartedauer ggü. dem Fachdienst fest.
ReadTimeout	60 Sekunden	Legt die Wartedauer für Leseoperatoinen ggü. dem Fachdienst fest.
AuthMode	SRV	Legt fest, wie sich das Clientmodul ggü. dem MTA authentifiziert. Möglicher Wert ist SRV.
SSLEnabledProtocols	TLSv1.2	Legt die möglichen Versionen des Verschlüsselungsprotokolls zum MTA fest.
CipherSuites	Siehe Anhang A.4 „Liste verwendeter Cipher-Suiten"	Durch das Clientmodul unterstützte Ciphersuites in Richtung Fachdienst.
Keystore	type="PKCS12" <absoluter Pfad>\ clientmodule_keystore.p12	Legt die Bezeichnung des verwendeten Schlüsselspeichers fest. Der Parameter „type" muss dem Keystore-Typen entsprechen (hier also „PKCS12").

Name	Default-Wert	Beschreibung
KeystorePass-word	ENC(…)	Beinhaltet das Kenn-wort zum Schlüssel-speicher.
KeyAlias	<Rechnername>	Beinhaltet einen Alias-Namen für den Schlüssel des Clien-tmoduls.
KeyPassword	ENC(…)	Beinhaltet das Kenn-wort zum Schlüssel.

Tabelle 16: Parameterliste MailTransferAgent - Connection

4.6.7 Parameterliste Connectors

Name	Default-Wert	Beschreibung
defaultId	Konnektor	Bezeichnung des Standardkonnektors
Connector	-	Siehe Kapitel 4.6.7.1

Tabelle 17: Parameterliste Connectors

4.6.7.1 Unterparameter Connector

Name	Default-Wert	Beschreibung
adminUrl	-	URL zum Zugang zur Administrationsoberflä-che des Konnektors
id	-	IP-Adresse des Konnektors
password	ENC(…)	Beinhaltet das Anmel-dekennwort
user	-	Benutzername
Contexts	-	Siehe Kapitel 4.6.7.1.1
Soap	-	Siehe Kapitel 4.6.7.1.3
Ldap	-	Siehe Kapitel 4.6.7.1.5

Tabelle 18: Parameterliste Connector

4.6.7.1.1 Unterparameter Contexts

Name	Default-Wert	Beschreibung
autoDiscovery	true	-
defaultId	Context1	Bezeichner des Default-Kontextes
Context	-	Siehe Kapitel 4.6.7.1.2

Tabelle 19: Parameterliste Connector/Contexts

4.6.7.1.2 Unterparameter Context

Name	Default-Wert	Beschreibung
id	Context1	Eindeutiger Name für einen Aufrufkontext innerhalb des Konnektors
MandantId	-	Bildet die Mandanten-ID ab.
ClientSystemId	-	Bildet die Clientsystem-ID ab.
WorkPlaceId	-	Bildet die Workplace-ID ab.
UserId	-	Bildet die User-ID ab.

Tabelle 20: Parameterliste Connector/Contexts

4.6.7.1.3 Unterparameter Soap

Name	Default-Wert	Beschreibung
ServiceLoggingEnabled	false	Parameter, der das Schreiben der SOAP-Nachrichten in das KIM-Client-log ermöglicht.
ServiceSchemaValidation	false	Parameter, der das Überprüfen von SOAP-Nachrichten gegen ein Schema ermöglicht.
DVDUri	https://<Konnektor-IP-Adresse>/connector.sds	URI, die es ermöglicht, den Dienste-verzeichnisdienst des Konnektors abzurufen.
MTOMEnabled	false	Legt die Nutzung von MTOM für SOAP-Nachrichten fest.
SupportECC	false	Legt fest, ob ECC-Zertifikate genutzt werden sollen oder nicht.
Connection	-	Siehe Kapitel 4.6.7.1.4

Tabelle 21: Parameterliste Connector/Soap

4.6.7.1.4 Unterparameter Soap/Connection

Name	Default-Wert	Beschreibung
UseOpensslProvider	false	Legt das Verhalten zur Nutzung von Openssl fest.
Proxy	enabled = „false“ http = „true“ password = „“ socks = „false“ user = „“	Parametersatz, der die SOAP-Schnittstelle zum Konnektor definiert.
ConnectTimeout	10 sec	Legt die Wartezeit für Verbindungsversuche zum Konnektor fest.
ReadTimeout	60 sec	Legt die Wartezeit für Leseversuche zum Konnektor fest.
AuthMode	NONE	Legt fest, wie sich das Clientmodul ggü. dem Konnektor authentifiziert. Mögliche Werte: NONE, SRV, C_BASIC
BasicAuth	Password = „“ User = „“	Stellt die Parameter Benutzername und Kennwort für eine Basisauthentifizierung zum Konnektor bereit. Wird nur in Verbindung mit „AuthMode“ = C_BASIC verwendet.
SSLEnabledProtocols	TLSv1.2	Legt die möglichen Versionen des Verschlüsselungsprotokolls zum Konnektor fest.
CipherSuites	Siehe Anhang A.4 „Liste verwendeter Cipher-Suiten”	Durch das Clientmodul unterstützte Ciphersuites in Richtung Konnektor.

DisableCNCheck	true	Ermöglicht, die Überprüfung des Hostnamens (common name) abzuschalten.
Keystore	type="PKCS12" -	Legt die Bezeichnung des verwendeten Schlüsselspeichers fest. Der Parameter „type" muss dem Keystore-Typen entsprechen (hier also „PKCS12").
KeystorePassword	-	Beinhaltet das Kennwort zum Schlüsselspeicher.
KeyAlias	valid	Beinhaltet einen Alias-Namen für den Schlüssel des Clientmoduls.
KeyPassword	-	Beinhaltet das Kennwort zum Schlüssel.
Truststore	type="PKCS12" connector.p12	Legt die Bezeichnung des verwendeten Zertifikatsspeichers fest. Der Parameter „type" muss dem Truststore-Typen entsprechen (hier also PKCS12).
TruststorePassword	ENC(…)	Beinhaltet das Kennwort zum Zertifikatsspeicher.

Tabelle 22: Parameterliste Connector/Soap/Connection

4.6.7.1.5 Unterparameter Ldap

Name	Default-Wert	Beschreibung
AllowAnonymous	true	Ermöglicht eine anonyme Verbindung zum VZD, d.h., ohne Authentifizierung. Mögliche Werte: False, True
User	-	Ermöglicht die Hinterlegung eines Benutzernamens für die Anmeldung am VZD.
Password	-	Ermöglicht die Hinterlegung eines Kennworts für die Anmeldung am VZD.
BaseDn	dc=data,dc=vzd	Legt die Werte für die Domänenkomponente fest.
Scope	one	Legt in der Baumstruktur eines LDAP den Suchbereich unter der Ebene BaseDn fest.
Connection		Siehe Kapitel 4.6.7.1.6

Tabelle 23: Parameterliste Connector/Ldap

4.6.7.1.6 Unterparameter Ldap/Connection

Name	Default-Wert	Beschreibung
Host	-	IP-Adresse des Konnektors
Port	389	Port, über den die LDAP-Anfragen an den Konnektor übermittelt werden. Für LDAPs Port 636.
Proxy	Password = „“ User = „“	Parametersatz, der die LDAP-Schnittstelle zum Konnektor definiert.
ConnectTimeout	10 sec	Legt die Wartezeit für Verbindungsversuche zum Konnektor für LDAP-Anfragen fest.
ReadTimeout	30 sec	Legt die Wartezeit für Leseversuche zum Konnektor für LDAP-Anfragen fest.
AuthMode	NONE	Legt fest, wie sich das Clientmodul ggü. dem Konnektor für LDAP-Anfragen authentifiziert. Mögliche Werte: NONE, SRV
SSLEnabledProtocols	TLSv1.2	Legt die möglichen Versionen des Verschlüsselungsprotokolls zum Konnektor fest.
CipherSuites	Siehe Anhang A.4 „Liste verwendeter Cipher-Suiten”	Durch das Clientmodul unterstützte Ciphersuiten in Richtung Konnektor für LDAP-Kommunikation.

Keystore	- type="PKCS12"	Legt die Bezeichnung des verwendeten Schlüsselspeichers fest. Der Parameter „type" muss dem Keystore-Typen entsprechen (hier also PKCS12).
KeystorePassword	-	Beinhaltet das Kennwort zum Schlüsselspeicher.
KeyAlias	valid	Beinhaltet einen Alias-Namen für den Schlüssel des Clientmoduls.
KeyPassword	ENC(…)	Beinhaltet das Kennwort zum Schlüssel.
Truststore	type="PKCS12" connector.p12	Legt die Bezeichnung des verwendeten Zertifikatsspeichers fest. Der Parameter „type" muss dem Truststore-Typen entsprechen (hier also PKCS12).
TruststorePassword	ENC(…)	Beinhaltet das Kennwort zum Zertifikatsspeicher.

Tabelle 24: Parameterliste Connector/Ldap/Connection

4.6.8 Parameterliste KIMContextRuleMapping

Name	Default-Wert	Beschreibung
enabled	true	Wenn auf true, wird das Rule-Mapping berücksichtigt, ansonsten false.
Always	false	Wenn auf false, wird das Rule-Mapping nur genutzt, wenn im Benutzernamen kein Kontext vorhanden ist. Wenn auf true, wird das Rule-Mapping immer genutzt.
KIMContextRules	id="Rules1"	Siehe Kapitel 4.6.8.1
DefaultSmtpKIM-ContextRule	context="…"	Definiert eine Default-Regel auf Basis der bei der Installation konfigurierten Parameter für SMTP.
DefaultPop3KIM-ContextRule	context="…"	Definiert eine Default-Regel auf Basis der bei der Installation konfigurierten Parameter für POP3.

Tabelle 25: Parameterliste KIMContextRuleMapping

4.6.8.1 Unterparameter KIMContextRules

Hinweis: Zum Einsatz und den Konfigurationsmöglichkeiten des KIM-Kontextmappings siehe auch Kapitel 4.3.7.

Name	Default-Wert	Beschreibung
ConnectorStrategy	type="single" -	IP-Adressen der Konnektoren, für die die Konnektorstrategie gilt (1 .. n). Die Angabe der IP-Adressen erfolgt kommasepariert. Parameter „type": Mögliche Werte: „single", „roundrobbin" „single" entspricht der Nutzung eines einzelnen Konnektors. „roundrobbin" setzt die Nutzung von mindestens zwei Konnektoren voraus.
KIMContextRule	context="…" id="…" protocol="…" -	E-Mail-Adresse, für die die Regel gelten soll. Weitere Parameter: „context" bezeichnet den Aufrufkontext, wie er lt. Regel verwendet werden soll. „id" entspricht dem Namen der Regel. „protocol" bildet das verwendete Protokoll für die Regel ab. Werte sind „smtp" oder „pop3".

Tabelle 26: Parameter KIMContextRuleMapping/KIMContextRules

4.6.9 Parameterliste AdminClient

Name	Default-Wert	Beschreibung
enabled	true	Definiert die Sichtbarkeit des Admin-Clients in der Taskleiste. „true": Admin-Client ist sichtbar. „false": Admin-Client ist nicht sichtbar.
MinPassword-Length	12	Legt die minimale Kennwortlänge fest.

Tabelle 27: Parameterliste AdminClient

4.6.10 Parameterliste RestAPI

Name	Default-Wert	Beschreibung
enabled	false	Definiert die Verfügbarkeit der REST-Schnittstelle für nutzende Systeme
ApiKey	01234-56789	Legt einen Schlüssel fest, der für die Nutzung der REST-API zur Identifikation übermittelt wird.
RestServer	-	Siehe hierzu Kapitel 4.6.10.1.

Tabelle 28: Parameterliste RestApi

4.6.10.1 Unterparameter RestServer

Name	Default-Wert	Beschreibung
RestHostname	Localhost	Hostname oder IP-Adresse, unter denen der Rest-Server erreichbar ist.
RestPort	8080	Port unter dem der Rest-Server auf dem Host erreichbar ist.
RestTimeout	5 min	Time-Out-Zeit bis zum Schließen der Verbindung.
Connection	-	Siehe hierzu Kapitel 4.6.10.2.

Tabelle 29: Parameterliste RestServer

4.6.10.2 Unterparameter RestServer/Connection

Name	Default-Wert	Beschreibung
AuthMode	NONE	Legt fest, wie sich das Clientmodul ggü. dem REST-Server authentifiziert. Mögliche Werte: NONE, SRV, C_X509.
SSLEnabledProtocols	TLSv1.2	Legt die möglichen Versionen des Verschlüsselungsprotokolls zum REST-Server fest.
CipherSuites	Siehe Anhang A.4 „Liste verwendeter Cipher-Suiten”	Durch das Clientmodul unterstützte Ciphersuiten in Richtung REST-Schnittstelle
Keystore	Type=“PKCS12“ <Pfad>/clientmodule_keystore.p12	Vollqualifizierter Pfad zum Schlüsselspeicher. Der Parameter „type“ muss dem Keystore-Typen entsprechen (hier also PKCS12).
KeystorePassword	ENC(…)	Beinhaltet das Kennwort zum Schüsselspeicher
KeyAlias	<Rechnername>	Beinhaltet den Alias
KeyPassword	ENC(…)	Beinhaltet das Kennwort zum Schlüssel
Truststore	Type=“PKCS12“ -	Legt die Bezeichnung des verwendeten Zertifikasspeichers fest. Der Parameter „type“ muss dem Truststore-Typen entsprechen (hier also PKCS12).
TruststorePassword	ENC(…)	Beinhaltet das Kennwort zum Zertifikatsspeicher.
EnableTLSClientAuth	False	Definiert die TLS-Clientauthentifizierung ggü. dem REST-Server

Tabelle 30: Parameterliste RestServer

4.6.11 Parameterliste Mailcache

Name	Default-Wert	Beschreibung
enabled	false	Steuert die Nutzung und die Anbindung des Mailcaches. „false“: Mailcache wird nicht genutzt. „true“: Mailcache wird genutzt.
Url	-	Beinhaltet die URL unter der der Mailcache erreichbar ist.
Connection	-	Siehe Kapitel 4.6.11.1

Tabelle 31: Parameterliste Mailcache

4.6.11.1 Unterparameter Connection

Name	Default-Wert	Beschreibung
AuthMode	NONE	Legt fest, wie sich der KIM-Client ggü. dem Mailcache authentifiziert. Mögliche Werte: NONE, SRV
SSLEnabledProtocols	TLSv1.2	Legt die möglichen Versionen des Verschlüsselungsprotokolls zum Mailcache fest.
CipherSuites	Siehe Anhang A.4 „Liste verwendeter Cipher-Suiten”	Durch das Clientmodul unterstützte Ciphersuites in Richtung Konnektor.
Keystore	type=“PKCS12“ -	Legt die Bezeichnung des verwendeten Schlüsselspeichers fest. Der Parameter „type“ muss dem Keystore-Typen entsprechen (hier also „PKCS12“)
KeystorePassword	-	Beinhaltet das Kennwort zum Schlüsselspeicher.
KeyAlias	-	Beinhaltet einen Alias-Namen für den Schlüssel des Clientmoduls.
KeyPassword	-	Beinhaltet das Kennwort zu Schlüssel.
Truststore	Type=“PKCS12“ Mailcache_truststore.p12	Legt die Bezeichnung des verwendeten Zertifikasspeichers fest. Der Parameter „type“ muss dem Truststore-Typen entsprechen (hier also PKCS12).
TruststorePassword	ENC(…)	Beinhaltet das Kennwort zum Zertifikatsspeicher.

Tabelle 32: Unterparameter Connection

4.6.12 Parameterliste AntiVirusEngines

Name	Default-Wert	Beschreibung
activeEngine	AMSI	Legt die Art der AV-Scanner-Unterstützung fest. Mögliche Werte sind AMSI, ClamAVTCPClient
enabled	False	Legt fest, ob ein Virenscanner eingebunden werden soll: true = wird eingebunden false = wird nicht mit eingebunden
pop3	True	Nutzung eines eingebundenen Virenscanners zur Überwachung des POP3-Verkehrs.
smtp	True	Nutzung eines eingebundenen Virenscanners zur Überwachung des SMTP-Verkehrs.
AMSI	-	Siehe Kapitel 4.6.12.1.
ClamAVTCPClient	-	Siehe Kapitel 4.6.12.2.

Tabelle 33: Parameterliste AntiVirusEngine

4.6.12.1 Unterparameter AMSI

Der Unterparameter AMSI besitzt keine weiteren Einstellungsmöglichkeiten. Der Knoten bleibt daher leer.

4.6.12.2 Unterparameter ClamAVTCPClient

Name	Default-Wert	Beschreibung
Hostname	Localhost	URL des Hosts, auf dem ClamAV ausgeführt wird.
Port	3310	Port, über den ClamAV erreichbar ist.
ConnectTimeout	10 Sekunden	Dauer bis zum Schließen einer ungenutzten Verbindung.
ReadTimeout	10 Sekunden	Dauer bis zum Abbruch eines Lesevorgangs ohne Datenübertragung.

Tabelle 34: Unterparameter ClamAVTCPClient

4.6.12.3 Unterparameter ICAPClient

Name	Default-Wert	Beschreibung
Hostname	Localhost	URL des Hosts, auf dem der ICAP-Server ausgeführt wird.
Port	1344	Port, über den der ICAP-Server erreichbar ist.
Servicename	Virus_scan	Bezeichnung für den Dienst, der genutzt wird
Secure	False	Legt die Verwendung von serverseitigem TLS fest: True = Verwendung von TLS False = Keine Verwendung von TLS
ConnectTimeout	10 Sekunden	Dauer bis zum Schließen einer ungenutzten Verbindung.
ReadTimeout	10 Sekunden	Dauer bis zum Abbruch eines Lesevorgangs ohne Datenübertragung.

Tabelle 35: Unterparameter ICAPClient

4.7 Ergänzende Betrachtungen zur konfigurativen Erweiterung der lokalen PKI

4.7.1 Grundsätzliches

Grundlegende Einstellungen zur lokalen PKI werden bereits während der Installation durchgeführt. Spätere Änderungen sind durch Anpassungen an der clientmodule.xml möglich. In den nachfolgenden Kapiteln werden beispielhaft Szenarien und deren Konfiguration dargestellt. Einstellungen in eckigen Klammern (<>) entsprechen individuellen Parametern.

4.7.2 TLS zum Konnektor nur mit Serverzertifikat

- Konfigurieren Sie den Konnektor so, dass die lokale Kommunikation TLS verwendet.
- Ändern Sie in der clientmodule.xml den Parameter Connector→Soap→Connection→AuthMode auf SRV

4.7.3 TLS zum Konnektor mit Benutzername und Kennwort

- Konfigurieren Sie den Konnektor so, dass dieser ein bestimmten Benutzernamen und ein Kennwort für die TLS-Authentifizierung erwartet.
- Ändern Sie in der clientmodule.xml den Parameter Connector→Soap→Connection→AuthMode auf C_BASIC
- Konfigurieren Sie den Parameter Connector→Soap→Connection→BasicAuth mit user=<Benutzername> und password=<Kennwort>

Tragen Sie das Kennwort im Klartext ein. Beim nächsten Starten wird das Kennwort verschlüsselt.

4.7.4 TLS zum Primärsystem oder E-Mail-Client nur mit Serverzertifikat

Vorbemerkung: Da das Primärsystem bzw. der E-Mail-Client die Verbindung zum KIM-Client aufbaut, nimmt der KIM-Client im Rahmen des TLS-Handshakes die Rolle des TLS-Servers ein und das Primärsystem bzw. der E-Mail-Client die des TLS-Clients.

- Konfigurieren Sie am Primärsystem bzw. E-Mail-Client die Verwendung von TLS.
- Ändern Sie in der clientmodule.xml den Parameter ClientSystem→Connection→AuthMode in „SRV“.

Als TLS-Serverzertifikat wird das Zertifikat verwendet, das für die Clientmodulinstallation konfiguriert wurde (Standard ist clientmodule_keystore.p12).

4.7.5 TLS zum Primärsystem oder E-Mail-Client mit Client- und Serverzertifikat I

Vorbemerkung: Da das Primärsystem bzw. der E-Mail-Client die Verbindung zum KIM-Client aufbaut, nimmt der KIM-Client im Rahmen des TLS-Handshakes die Rolle des TLS-Servers ein und das Primärsystem bzw. der E-Mail-Client die des TLS-Clients.

- Konfigurieren Sie am Primärsystem bzw. E-Mail-Client die Verwendung von TLS.
- Ändern Sie in der clientmodule.xml den Parameter ClientSystem→Connection→AuthMode in „C_X509“.

Der KIM-Client akzeptiert dann nur noch Clients, die ein TLS-Zertifikat präsentieren. Das TLS-Zertifikat ist in diesem Fall unspezifisch.

4.7.6 TLS zum Primärsystem oder E-Mail-Client mit Client- und Serverzertifikat II

Vorbemerkung: Da das Primärsystem bzw. der E-Mail-Client die Verbindung zum KIM-Client aufbaut, nimmt der KIM-Client im Rahmen des TLS-Handshakes die Rolle des TLS-Servers ein und das Primärsystem bzw. der E-Mail-Client die des TLS-Clients.

- Konfigurieren Sie am Primärsystem bzw. E-Mail-Client die Verwendung von TLS.
- Ändern Sie in der clientmodule.xml den Parameter ClientSystem→Connection→AuthMode in „C_X509“.
- Geben Sie unter ClientSystem→Connection→Truststore den Namen des zu verwendenden Truststores an, und speichern Sie die Truststore-Datei im Konfigurationsverzeichnis ab. Geben Sie unter type den Typ des Truststores an, im Regelfall PKCS12.
- Geben Sie unter ClientSystem→Connection→TruststorePasswort das zum Öffnen des Truststores notwendige Kennwort im Klartext an. Nach erneutem Start des KIM-Clients wird das Passwort automatisch verschlüsselt gespeichert. Die Verschlüsselung erkennen Sie an der kryptischen Darstellung des Passworts, der ein ENC vorangestellt ist.

Der KIM-Client akzeptiert dann nur noch Clients, die ein TLS-Zertifikat präsentieren. Das vom Client präsentierte TLS-Zertifikat muss im Truststore des KIM-Clients enthalten sein.

4.7.7 Nutzung von LDAPs

Wichtiger Hinweis:

Für die Nutzung von LDAP im Wirkbetrieb ist durch gematik festgelegt worden, dass diese ausschließlich via TLS erfolgen muss. Des Weiteren darf eine Client-Authentifizierung ausschließlich mittels Zertifikats erfolgen. Es kann jedoch auch auf eine Client-Authentifizierung verzichtet werden.

Siehe hierzu gemSpec_CM_KOMLE, Anforderung A_21223-01.

Es ist möglich, das Adressbuch auf LDAPs umzustellen. Dazu gehen Sie wie folgt vor:

- Konfigurieren Sie am Primärsystem bzw. E-Mail-Client die Verwendung von LDAPs. Der hierfür standardisiert verwendete Port ist 636.
- Ändern Sie in der clientmodule.xml den Parameter Connector→LDAP→Connection→Ports auf den verwendeten Port (i.a. 636).
- Passen Sie die Client-Authentifizierung den Einstellungen am Konnektor an.

Hinweis zum Multikonnektor-Support:

Das Adressbuch ist konnektorspezifisch und kann für jeden Konnektor individuell konfiguriert werden.

4.8 Fehlerbehebung und Auswertung von Logs

4.8.1 Fehlerbehebung

Anwendungsfehler sind bisher nicht bekannt.

4.8.2 Auswertung von Logs

Auftretende Probleme werden in Logdateien protokolliert.

Folgende Logdateien sind für die Problembehandlung verfügbar:

- *clientmodule.log*
- *clientmoduleError.log*

Diese Dateien befinden sich im Verzeichnis „logs“ das direkt unter dem Installationsverzeichnis der Anwendung liegt.

Ergänzend hierzu findet sich im Stammverzeichnis der Installation die Datei „errorLog“. Sie protokolliert Fehler mit, die eine direkte Ausführung der Anwendung verhindern.

Zusätzlich zu den Logdateien zur Problembehandlung findet sich im Ordner „logs“ die Datei

- *performance.log*

Diese Datei gibt Auskunft über die Verarbeitungszeiten von Nachrichten.

4.9 Datensicherung

Eine durch die Anwendung automatisierte Datensicherung findet nicht statt. Ist eine Datensicherung Ihrerseits erforderlich, so ist diese entweder von Hand in regelmäßigen Abständen – zumindest nach Änderung – oder aber mittels Cronjob o. ä. durchzuführen.

Es wird empfohlen, die Logdateien sowie die Konfigurationsdatei in regelmäßigen Abständen zu sichern. Ebenfalls ist es empfehlenswert, eine Sicherung vor Deinstallation oder Aktualisierung durchzuführen.

Weitere Daten werden von der Anwendung nicht gespeichert und sind daher auch nicht zu sichern.

4.10 Bekannte Fehler, Workarounds und Problembehandlung

4.10.1 Bekannte Fehler

Fehler sind zurzeit nicht bekannt.

4.10.2 Workarounds

Workarounds werden zurzeit nicht angeboten.

4.10.3 Problembehandlung

Problem	Mögliche Ursache	Workaround
E-Mail kann nicht signiert werden.	Die SMC-B ist nicht verifiziert.	Verifizieren Sie die SMC-B und wiederholen den Vorgang erneut.
Timeout des E-Mail-Clients beim Empfang von Mails	Die Verarbeitungszeit zum Empfangen von Mails, insbesondere mit großem Anhang) verlängert sich durch Entschlüsseln und Signaturprüfung derart, dass der E-Mail-Client in ein Timeout läuft.	In Thunderbird kann das Timeout erhöht werden (Standard ist 100 Sekunden). Die Anpassung der Konfiguration erfolgt über: Extra→Einstellungen→Allgemein→Konfiguration bearbeiten… Verifiziert unter Thunderbird V78.x Dort wird folgender Eintrag hinzugefügt: „mail.server.serverXX.timeout“. Die Wertangabe erfolgt in Sekunden. „XX“ ist der (numerische) Platzhalter für den Server. Dieser Wert gilt nur für den ausgewählten Server. Verifiziert unter Thunderbird V91.3.0 und V102.12.0 Suchen Sie nach dem Eintrag „mailnews.tcptimeout“. Die Wertangabe erfolgt in Sekunden. Dieser Wert gilt für alle in Thunderbird konfigurierten Konten. Outlook In Outlook lässt sich ebenfalls das Timeout anpassen. Die Konfigurationswege unterscheiden sich jedoch von Version zu Version. Konsultieren Sie hierzu daher die entsprechende Dokumentation des Herstellers.
Timeout des E-Mail-Servers beim Senden von Mails	Blacklist/Whitelist bzw. BPjM des Virenprogramms sind aktiv.	Prüfen Sie, ob Einstellungen bzgl. Blacklist/Whitelist bzw. BPjM den Zugriff auf den Server unterbinden, und ändern Sie ggf. Ihre Konfiguration.
Es werden keine Karten gefunden	Mandantenkontext nicht gültig.	Prüfen Sie zuerst, ob der Mandantenkontext den Anforderungen des KIM-Clients entspricht (nur Ziffern und Buchstaben). Prüfen Sie außerdem am Konnektor, ob dem Mandantenkontext Karten zugeordnet sind.
Probleme beim Finden von Zertifikaten im VZD	Zertifikatscache arbeitet ggf. im Konnektorkontext nicht richtig.	Setzen Sie in der Datei „clientmodule.xml“ den Parameter „ClientModule→EncCertCacheAlivePeriod“ auf den Wert „0“. Speichern Sie danach die Datei und starten dann das Clientmodul neu.

Tabelle 36: Problembehandlung

5 E-Mail-Client-Konfiguration

5.1 Vorbemerkung

Im Zuge der Verwendung des KIM-Clientmoduls sind in den vorhandenen E-Mail-Clients die KIM-E-Mail-Adressen einzurichten. Darüber hinaus können an den nutzenden Systemen Optimierungen vorgenommen werden, die die Arbeit mit KIM erleichtern.

Dieses Kapitel soll einen Überblick zur grundlegenden Einrichtung eines E-Mail-Postfachs am Client und die Optimierungsmöglichkeiten geben. Dabei ist jedoch zu beachten, dass aufgrund der Vielzahl von verschiedenen E-Mail-Clients die Vorgehensweisen und Möglichkeiten nur beispielhaft aufgezeigt werden können.

Es ist nicht auszuschließen, dass Ihr E-Mail-Client bestimmte Funktionen nicht unterstützt oder auf andere Art zur Verfügung stellt.

Bei Fragen zu Ihrem E-Mail-Client, dessen Leistungsumfang und ggf. die Umsetzung von Optimierungen wenden Sie sich bitte an Ihren IT-Dienstleister.

Wichtiger Hinweis:

Bitte denken Sie daran, dass Sie für die Adressierung von HBA den vollständigen Aufrufkontext einschließlich userID benötigen.

5.2 Einrichten einer E-Mail-Adresse

5.2.1 Erforderliche Daten

Für die Einrichtung des E-Mail-Clients benötigen Sie folgende Informationen:

- E-Mail-Adresse
- Passwort zur E-Mail-Adresse

Die E-Mail-Adresse und das dazugehörige Passwort haben Sie bei der Anlage des Kontos im Admin-Client (für Windows im Kapitel 4.3.1) registriert.

- Lokalen Port des KIM-Clients für SMTP (siehe Kapitel 4.6.3.1, SmtpPort)
- Lokalen Port des KIM-Clients für POP3 (siehe Kapitel 4.6.3.1, Pop3Port)
- IP-Adresse und Port des Fachdienstes für SMTP und POP3:

Umgebung	Dienst	IP	Port
RU	SMTP	10.30.1.132	465
	POP3	10.30.1.132	995
PU	SMTP	100.102.1.169	465
	POP3	100.102.1.169	995

Tabelle 37: Übersicht der IP- und Portinformationen zum Fachdienst

- Vollständigen Mandantenkontext

Die erforderlichen Daten sind unabhängig vom verwendeten E-Mail-Client.

5.2.2 Bildung des Benutzernamens

Der Benutzername in Ein-Konnektor-Umgebungen wird wie folgt gebildet:

SMC-B:

<E-Mail-Adresse>#<IP-Adresse des Fachdienstes>:< Port des Fachdienstes>#<Mandant>#<Client-System>#<Arbeitsplatz>

HBA:

<E-Mail-Adresse>#<IP-Adresse des Fachdienstes>:< Port des Fachdienstes>#<Mandant>#<Client-System>#<Arbeitsplatz>#<Benutzer>

In Multi-Konnektor-Umgebungen wird an den Benutzernamen noch der Ziel-Konnektor gehängt:

SMC-B:

<E-Mail-Adresse>#<IP-Adresse des Fachdienstes>:< Port des Fachdienstes>#<Mandant>#<Client-System>#<Arbeitsplatz>##<Konnektor>

Wichtiger Hinweis:
Bitte beachten Sie unbedingt, dass bei fehlendem Benutzernamen dieser trotzdem zu berücksichtigen ist und daher zwei Hash-Tags zwischen <Arbeitsplatz> und <Konnektor> vorzusehen sind.

HBA:

<E-Mail-Adresse>#<IP-Adresse des Fachdienstes>:< Port des Fachdienstes>#<Mandant>#<Client-System>#<Arbeitsplatz>#<Benutzer>#<Konnektor>

Port und IP-Adresse des Fachdienstes ermitteln Sie gemäß Kapitel 5.2.1.

Wichtiger Hinweis:
Achten Sie beim Benutzernamen unbedingt auf die einzufügenden Zeichen, wie Doppelpunkt zwischen IP-Adresse und Port, sowie die Doppelkreuze „#“ (Hash-Tags) als Abgrenzungszeichen.

Beispiele:

- Einkonnektorumgebung:
    - SMC-B-Benutzername für SMTP in der PU MVZHamburg@tsi.kim.telematik#100.102.1.169:465#Mandant1#CS1#AP1
    - SMC-B-Benutzername für POP3 in der PU MVZHamburg@tsi.kim.telematik#100.102.1.169:995#Mandant1#CS1#AP1

    - HBA-Benutzername für SMTP in der PU MVZHamburg@tsi.kim.telematik#100.102.1.169:465#Mandant1#CS1#AP1#U1
    - HBA-Benutzername für POP3 in der PU MVZHamburg@tsi.kim.telematik#100.102.1.169:995#Mandant1#CS1#AP1#U1
- Mehrkonnektorumgebung:
    - SMC-B-Benutzername für POP3 in der PU MVZHamburg@tsi.kim.telematik#100.102.1.169:995#Mandant1#CS1#AP1##konnektor2
    - HBA-Benutzername für POP3 in der PU MVZHamburg@tsi.kim.telematik#100.102.1.169:995#Mandant1#CS1#AP1#U1#konnektor2

Hinweis:
Für ein Konfiguration in der RU passen Sie die IP-Adresse des Benutzernamens an.

Um Ihnen die Bildung des Benutzernamens zu erleichtern, bietet Ihnen der KIM-Client die Möglichkeit, einen Benutzernamen generieren zu lassen, den Sie dann mittels Copy&Paste in Ihren E-Mail-Client übernehmen können.

Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie die Verwaltung (siehe Kapitel 4.3.3.1).
2. Geben Sie Ihre Konnektoreinstellungen an.
3. Wählen Sie per Doppelklick aus Account-Ansicht das E-Mail-Account aus, für das Sie einen E-Mail-Client einrichten wollen.
4. Ergänzen Sie die KIM-Anmeldedaten um das Kennwort.
5. Drücken Sie rechts neben der KIM-Adresse auf „KIM-Benutzername“.

Es öffnet sich ein Fenster, das Ihnen sowohl für SMTP als auch POP3 einen generierten Benutzernamen bereitstellt. Diesen können Sie in die Zwischenablage kopieren und von dort aus in das E-Mail-Clientprogramm mittels Strg-V übernehmen:

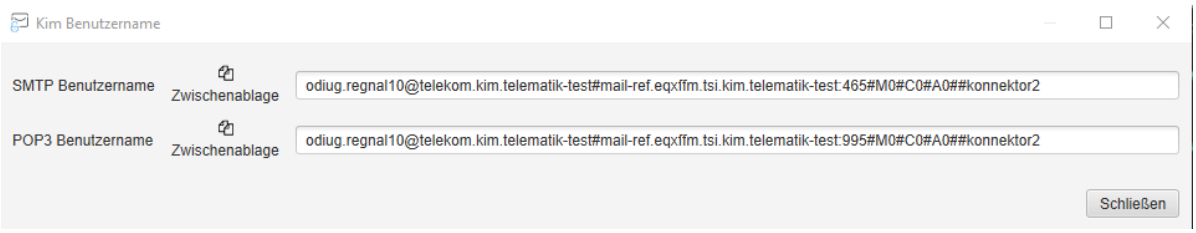

Abbildung 68: Generierter KIM-Benutzername zur Weiterverwendung im Primärsystem

5.2.3 Zentrales Adressbuch der TI

Die Telematikinfrastruktur verfügt über ein zentrales Adressbuch, das für KIM genutzt werden kann. Dieses Adressbuch ist der zentralen TI-Komponente Verzeichnisdienst (VZD) zugeordnet und LDAP-basiert.

Um das zentrale Adressbuch von Ihrem E-Mail-Client aus nutzen zu können, müssen Sie den LDAP-Client in Ihrem Clientprogramm konfigurieren.

Folgende Parameter sind zu konfigurieren:

Parameter	Wert
Name des Adressbuchs	z.B. TI_Adressbuch
Serveradresse[7]	z.B. 192.168.1.67
Basis-DN	dc=data,dc=vzd
Port-Nummer	389 (LDAP) oder 636 (LDAPs)

Tabelle 38: Parametertabelle für VZD-basiertes Adressbuch

5.2.4 Thunderbird

5.2.4.1 Vorbemerkung

Die nachfolgenden Kapitel wurden auf Thunderbird in folgenden Versionen getestet:

- 91.3.0 (64-Bit)
- 102.12.0 (64-bit)
- 102.14.0 (64-bit)
- 115.3.0 (64-bit) Supernova
- 115.7.0 (64-bit) Supernova

Neuere und auch ältere Versionen von Thunderbird können ggf. hiervon abweichen.

5.2.4.2 Konfiguration in Thunderbird

Um in Thunderbird eine KIM-E-Mail-Adresse einzurichten, gehen Sie wie folgt vor:

1. Gehen Sie in das Anwendungsmenü und wählen dort „Neu“ aus.
2. Rufen Sie dort „Bestehendes E-Mail-Konto …“ auf.

[7] Die Serveradresse entspricht der lokalen Konnektor-IP-Adresse.

Es wird ein Konfigurationsdialog gestartet.

3. Geben Sie die E-Mail-Adresse und das Passwort an.

Wichtiger Hinweis: Lassen Sie das Feld „Ihr Name“ unbedingt leer.

4. Drücken Sie den Button „Manuell einrichten“, um weitere Einstellungen vornehmen zu können.

Verwenden Sie folgende Parameter für POP3:

- Wählen Sie bei „Posteingangs-Server“ das Protokoll „POP3“ aus.
- Hostname: localhost (sofern auf demselben Host, wie Clientmodul) oder IP-Adresse des Clientmoduls
- Port: <POP3-Port des Clientmoduls>
- Verbindungssicherheit: SSL/TLS
- Authentifizierungsmethode: Passwort, normal
- Benutzername Posteingangs-Server: <E-Mail-Adresse>#<IP-Adresse des Fachdienstes>:<POP3-Port des Fachdienstes>#<Mandant>#<Client-System>#<Arbeitsplatz>

Um Ihnen die Bildung des Benutzernamens zu erleichtern, bietet Ihnen der KIM-Client die Möglichkeit, einen Benutzernamen generieren zu lassen, den Sie dann mittels Copy&Paste in Ihren E-Mail-Client übernehmen können. Lesen Sie hierzu Kapitel 5.2.2.

Verwenden Sie folgende Parameter für SMTP:

- Hostname: localhost (sofern auf demselben Host, wie Clientmodul) oder IP-Adresse des Clientmoduls
- Port: <SMTP-Port des Clientmoduls>
- Verbindungssicherheit: SSL/TLS
- Authentifizierungsmethode: Passwort, normal
- Benutzername Postausgangs-Server: <E-Mail-Adresse>#<IP-Adresse des Fachdienstes>:<SMTP-Port des Fachdienstes>#<Mandant>#<Client-System>#<Arbeitsplatz>

Um Ihnen die Bildung des Benutzernamens zu erleichtern, bietet Ihnen der KIM-Client die Möglichkeit, einen Benutzernamen generieren zu lassen, den Sie dann mittels Copy&Paste in Ihren E-Mail-Client übernehmen können. Lesen Sie hierzu Kapitel 5.2.2.

Drücken Sie „Erweiterte Einstellungen“ und bestätigen Sie den folgenden Dialog.

Das Konto wird in Thunderbird angelegt.

- In den Konten-Einstellungen wählen Sie links in der Übersicht der Konten das gerade angelegte E-Mail-Konto aus und drücken rechts in der Konfiguration „Postausgangs-Server (SMTP) bearbeiten …“.
- Vergeben Sie im nachfolgenden Dialog im Feld „Beschreibung“ einen eindeutigen Namen.

- Bestätigen Sie dann mit „OK“.

Im Feld „Postausgangs-Server (SMTP)“ wird dann die neue Beschreibung angezeigt.

Damit ist die Konfiguration abgeschlossen.

5.2.4.3 Adressbuch in Thunderbird

Den Namen des Adressbuchs aus Tabelle 38 können Sie frei wählen. In Abbildung 69 wurde das Adressbuch „VZD TU“ genannt. Die Abfrage des Adressbuchs erfolgt über die LDAP-Schnittstelle des Konnektors, deshalb entspricht die Serveradresse der IP-Adresse des Konnektors. Die Einträge für „Basis-DN“ sind verbindlich und dürfen nicht geändert werden.

Eine Adressbuchliste könnte dann so aussehen:

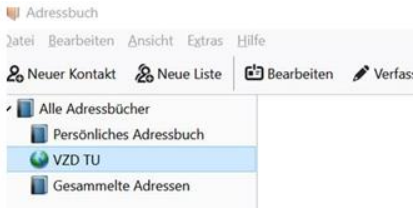

Abbildung 69: Beispiel für eine Adressbuchliste

Dieser Eintrag „VZD TU“ wäre dann bspw. folgendermaßen konfiguriert:

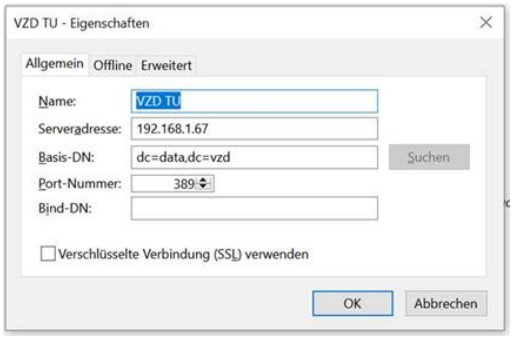

Abbildung 70: Beispiel für eine Adressbuchkonfiguration

5.2.5 Outlook

5.2.5.1 Vorbemerkungen

Die nachfolgend beschriebene Konfiguration von Outlook soll Ihnen einen groben Leitfaden an die Hand geben, wie Sie diesen E-Mail-Client für KIM nutzen können. Für über diesen Leitfaden hinaus gehende Informationen, insbesondere bzgl. Verschlüsselung, wenden Sie sich bitte an Ihren Administrator bzw. Systembetreuer.

Leider ist die Konfiguration von Outlook nicht einheitlich möglich. Je nach Systemausprägung bzw. Einstellungen Ihres Systemadministrators müssen Sie verschiedene Wege nutzen, um Outlook konfigurieren zu können.

Daher möchten wir Ihnen im Vorfeld drei verschieden Wege aufzeigen, wie Sie den gemeinsamen Einstiegspunkt für die Outlook-Konfiguration finden.

5.2.5.1.1 Aufruf über Systemsteuerung – Benutzerkonten – Mail (Microsoft Outlook)

- Rufen Sie die Systemsteuerung auf und wählen dort „Benutzerkonten“ aus:

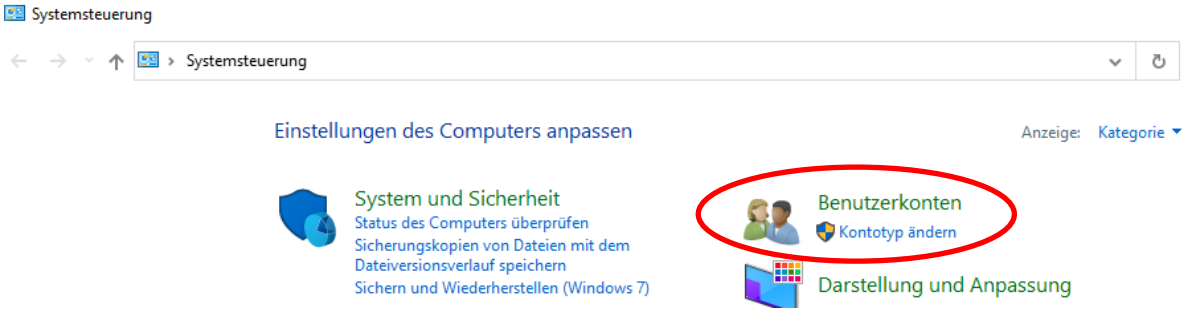

Abbildung 71: Systemsteuerung

- Wählen Sie „Mail (Microsoft Outlook)“ aus:

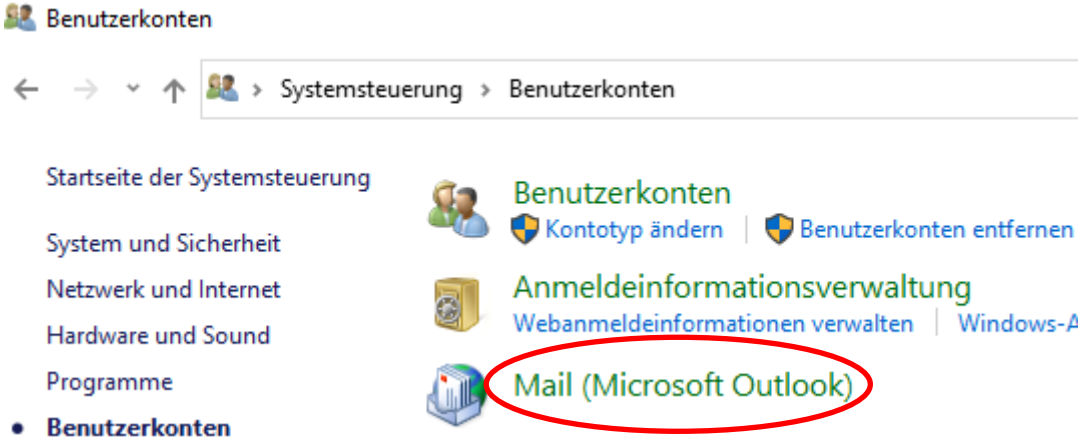

Abbildung 72: Systemsteuerung – Benutzerkonten

- Öffnen Sie die Anwendung „Mail (Microsoft Outlook)“.

Hinweis:

Der Eintrag „Mail (Microsoft Outlook)“ kann in Ihrer Installation vom Beispiel abweichen. Sie können sich jedoch am Icon  und „Mail“ orientieren.

- Öffnen Sie „Mail (Microsoft Outlook 2016)(32-bit)“.

  Es wird Ihnen der Konfigurationsdialog angezeigt:

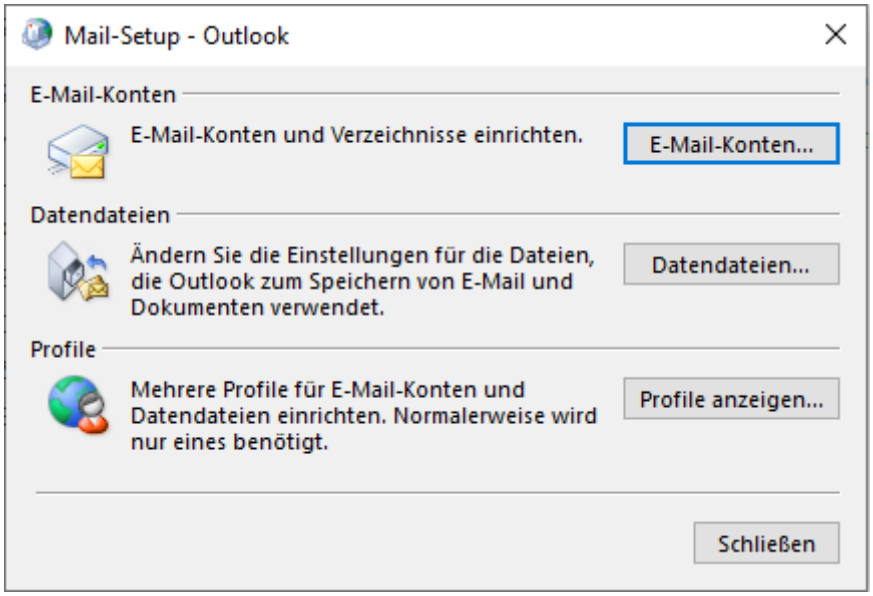

Abbildung 73: Dialog „Mail Setup – Outlook“

- Öffnen Sie dort den Eintrag „E-Mail-Konten …“.

Folgen Sie nun der weiteren Beschreibung in Kapitel 5.2.5.1.3.

5.2.5.1.2 Aufruf über Systemsteuerung – Mail (Microsoft Outlook) (32bit)

- Geben Sie in das Suchfeld der Windows-Taskleiste den Begriff „Systemsteuerung“ ein:

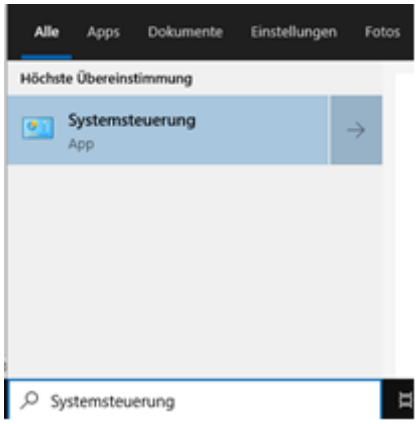

Abbildung 74: Systemsteuerung als Taskleisten-Suche

Klicken Sie auf das Ergebnis „Systemsteuerung“. Es öffnet sich die Systemsteuerung mit allen Steuerungselementen. Wählen Sie dort „Mail …“ aus:

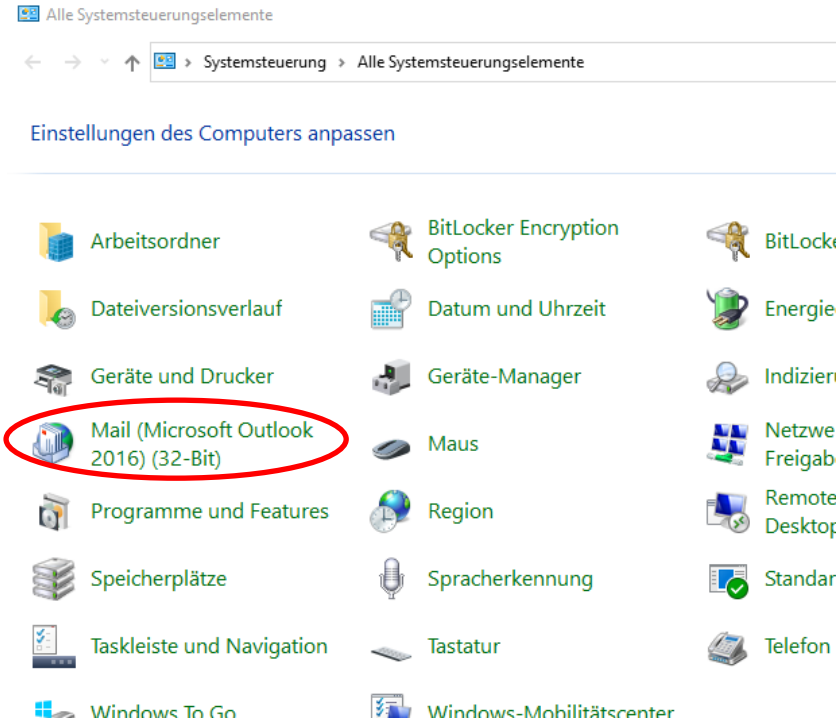

Abbildung 75: Systemsteuerung – Alle Systemsteuerungselemente

> Hinweis:
>
> Der Eintrag Mail „(Microsoft Outlook 2016)(32-bit)“ kann in Ihrer Installation vom Beispiel abweichen. Sie können sich jedoch am Icon  und „Mail“ orientieren.

- Öffnen Sie „Mail (Microsoft Outlook 2016)(32-bit)“.

  Es wird Ihnen der Konfigurationsdialog angezeigt:

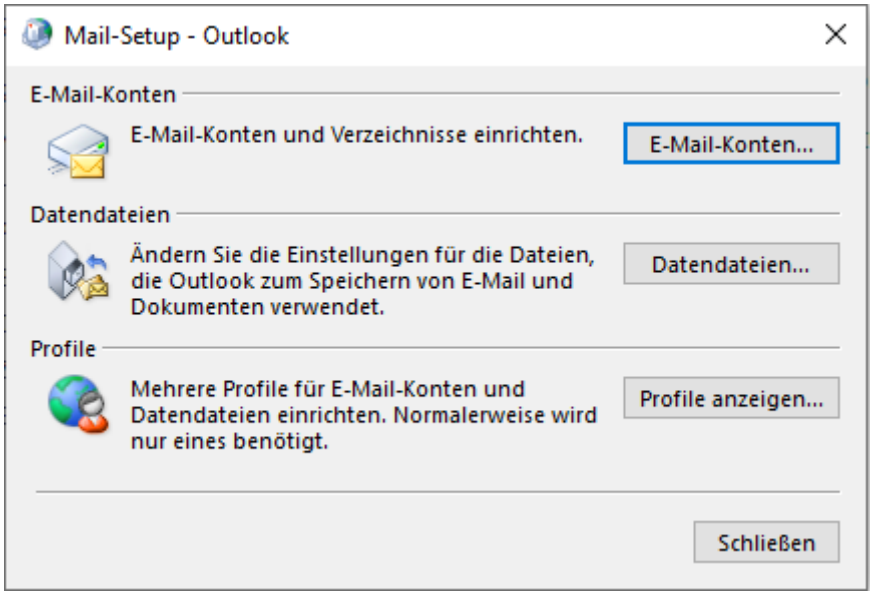

Abbildung 76: Dialog „Mail Setup – Outlook“

- Öffnen Sie dort den Eintrag „E-Mail-Konten …“.

Folgen Sie nun der weiteren Beschreibung in Kapitel 5.2.5.1.3.

5.2.5.1.3 Aufruf über den Outlook-Client

- Rufen Sie Ihren Outlook-Client auf.
- Wechseln Sie in das Menü „Datei“:

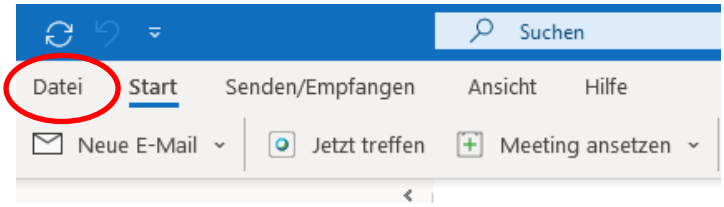

Abbildung 77: Menüeintrag Outlook-Datei

- Rufen Sie „Kontoeinstellungen“ auf und dort noch einmal „Kontoeinstellungen“:

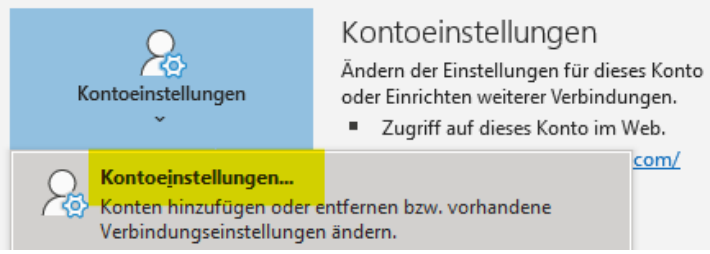

Abbildung 78: Outlook-Kontoeinstellungen

- Öffnen Sie die „Kontoeinstellungen“.

Folgen Sie nun der weiteren Beschreibung in Kapitel 5.2.5.1.3.

5.2.5.2 Konfiguration „Outlook-Kontoeinstellungen”

Die Konfiguration sieht folgendermaßen aus:

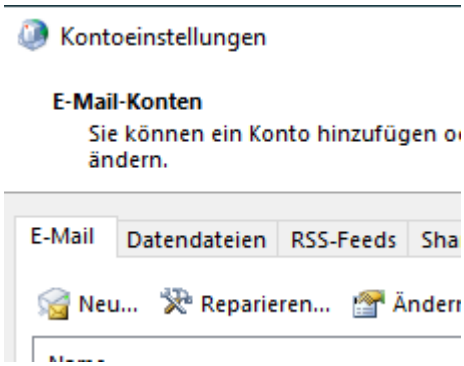

Abbildung 79: Outlook-Kontoeinstellungen

Wählen Sie den Karteireiter „E-Mail“. Dort klicken Sie auf „Neu …“. Es öffnet sich ein Einrichtungsassistent. Dieser ermöglicht Ihnen ein Konto hinzuzufügen. Wählen Sie die manuelle Konfiguration aus:

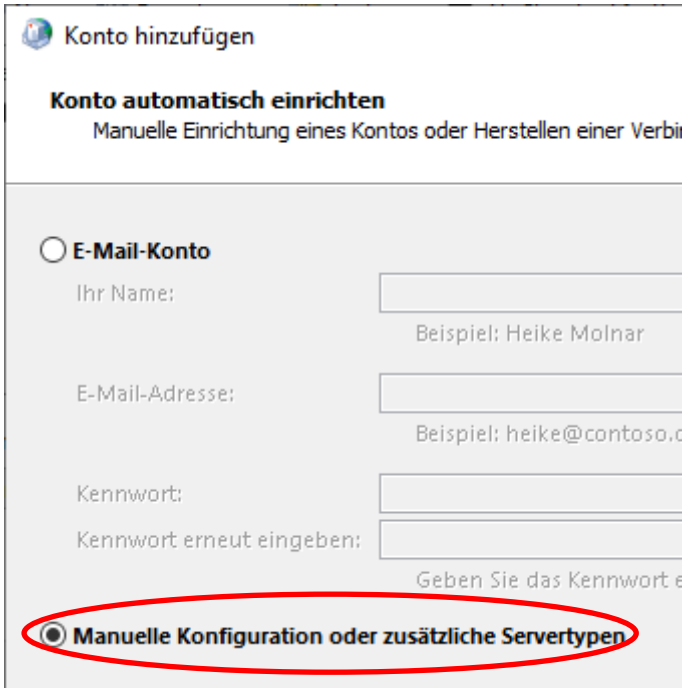

Abbildung 80: Dialog „Konto automatisch einrichten“

Drücken Sie „Weiter“. Wählen Sie im nachfolgenden Dialog die Auswahl „POP oder IMAP“ aus:

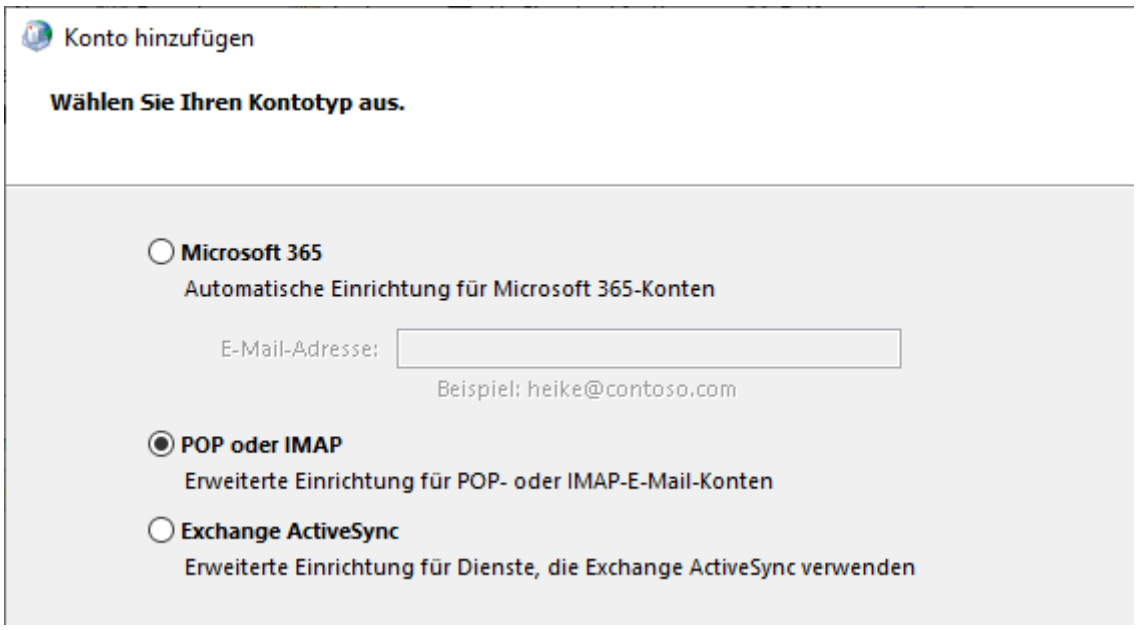

Abbildung 81: Dialog „Kontotyp“

Drücken Sie „Weiter“. Geben Sie im nachfolgenden Dialog die Kontodaten ein.

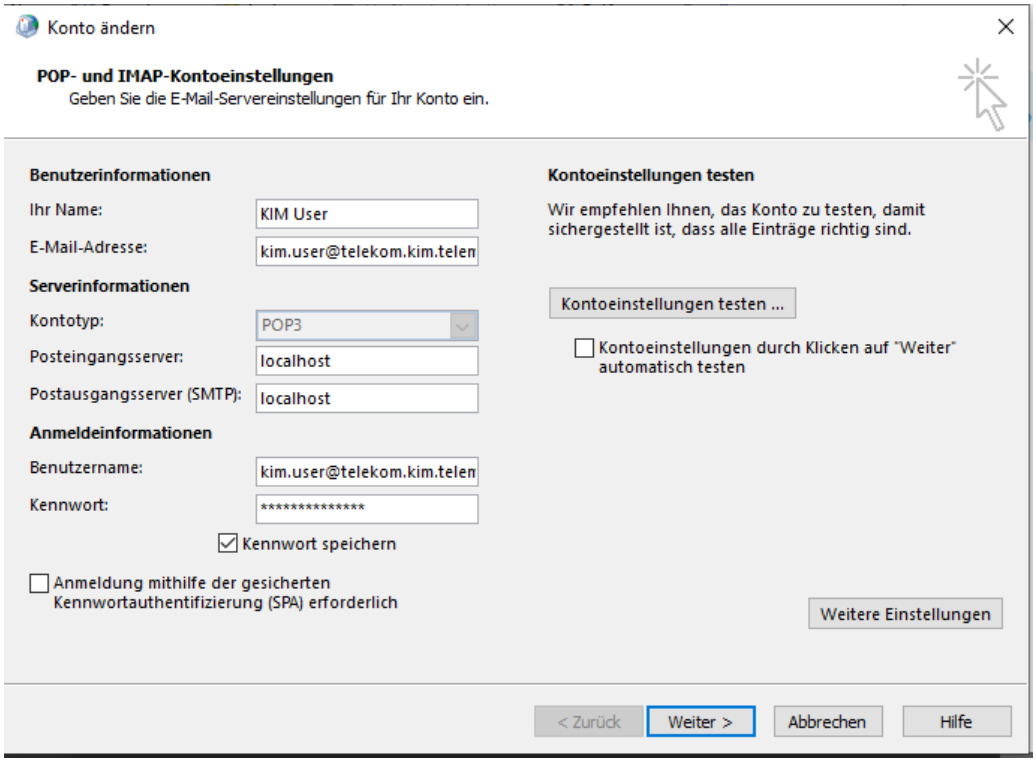

Abbildung 82: Dialog „POP- und IMAP-Kontoeinstellungen

Tragen Sie folgende Informationen ein:

- „Ihr Name“: Name des Kontos, wie er Ihnen in Outlook angezeigt werden soll.
- „E-Mail-Adresse“: KIM-E-Mail-Adresse
- Kontotyp: POP3
- Posteingangsserver: Sofern Outlook und KIM-Client auf demselben Server verwendet werden, können Sie „localhost“ eintragen. Wenn sich Outlook und KIM-Client auf unterschiedlichen Servern befinden, tragen Sie dort die IP-Adresse des KIM-Clients ein.
- Postausgangsserver: siehe „Posteingangsserver“.
- Benutzername: KIM-Benutzername, wie in Kapitel 5.2.1 „Erforderliche Daten“ beschrieben. Achten Sie auf den richtigen Port im Benutzernamen (>995<).
- Kennwort: Passwort zum KIM-Postfach.

Setzen Sie den Haken bei „Kennwort speichern“.

Hinweis:
Achten Sie darauf, dass bei „Kontoeinstellungen durch Klicken auf „Weiter“ automatisch testen“ kein Haken gesetzt ist.

Drücken Sie den Button „Weitere Einstellungen“.

Es öffnet sich der Dialog zur Konfiguration der Internet-E-Mail-Einstellungen. Wechseln Sie auf den Karteireiter „Postausgangsserver“:

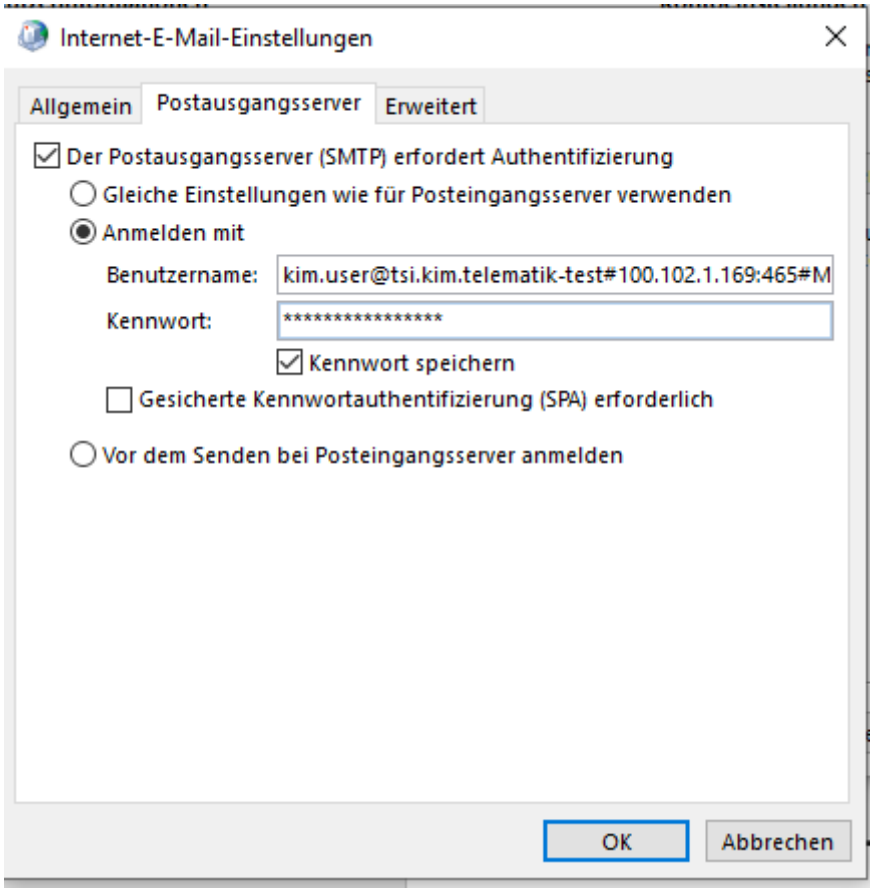

Abbildung 83: Internet-E-Mail-Einstellungen – Postausgangsserver

Tragen Sie folgende Informationen ein:

- Setzen Sie den Haken bei „Der Postausgangsserver (SMTP) erfordert Authentifizierung.
- Wählen Sie „Anmelden mit“ aus.
- Benutzername: KIM-Benutzername, wie in Kapitel 5.2.1 „Erforderliche Daten“ beschrieben. Achten Sie auf den richtigen Port im Benutzernamen (>465<).
- Kennwort: Passwort zum KIM-Postfach.

Setzen Sie den Haken bei „Kennwort speichern“.

Wechseln Sie nun auf den Karteireiter „Erweitert“:

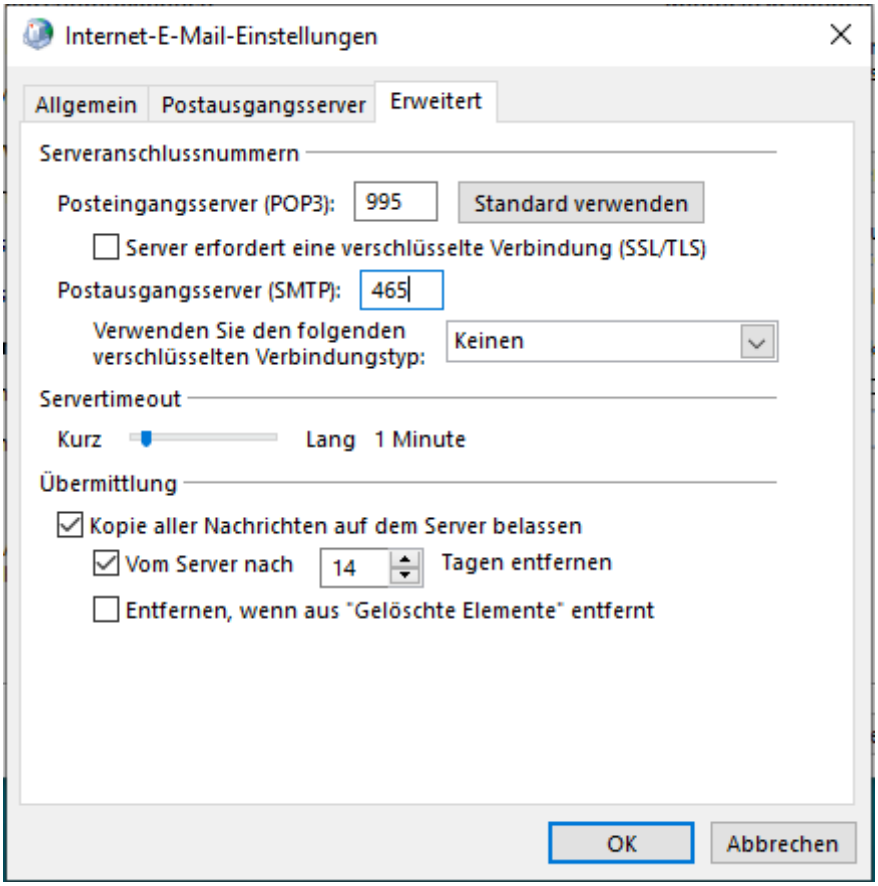

Abbildung 84: Internet-E-Mail-Einstellungen - Erweitert

Tragen Sie folgende Informationen ein:

- Posteingangsserver (POP3s): 995
- Postausgangsserver (SMTPs): 465

Damit ist die Konfiguration Ihres E-Mail-Kontos in Outlook abgeschlossen.

5.2.5.3 Adressbuch in Outlook

Um ein Adressbuch in Outlook zu konfigurieren, gehen Sie wie folgt vor:

- Öffnen Sie Ihren Outlook-Client
- Wählen Sie in der Menüzeile „Datei“ und dort „Kontoeinstellungen“ aus. Gehen Sie auf den Reiter „Adressbücher“:

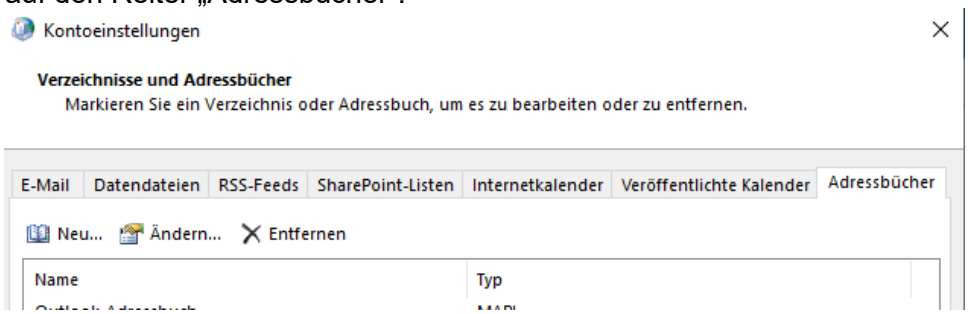

Abbildung 85: Outlook-Ausschnitt Kontoeinstellungen→Adressbücher

- Drücken Sie auf „Neu …“. Es wird der Assistent zum Hinzufügen eines Adressbuches gestartet. Wählen Sie „Internetverzeichnisdienst (LDAP)“ aus.

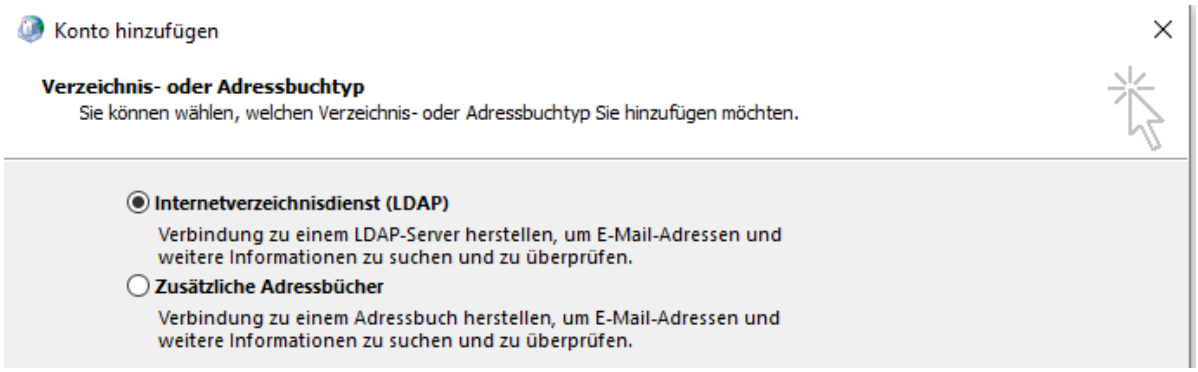

Abbildung 86: Outlook - Adressbuchtyp

- Konfigurieren Sie den Adressbuch-Server. Aus Sicht von Outlook stellt der Konnektor die Adressbuch-Funktionalität bereit. Konfigurieren Sie daher den Konnektor, indem Sie „konnektor“ als Servername eintragen.

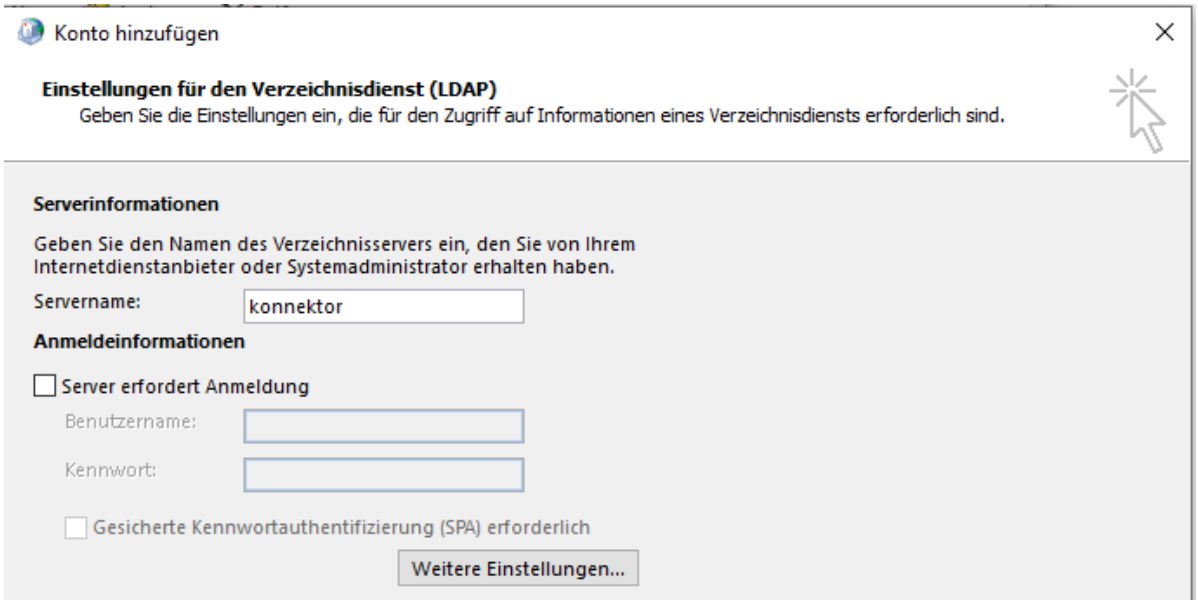

Abbildung 87: Outlook – Adressbuch-Server

> Hinweis:
>
> Markieren Sie „Server erfordert Anmeldung“ nebst Angabe von Benutzername und Kennwort, wenn Sie am Konnektor eine Clientsystem-Authentifizierung konfiguriert haben.

- Drücken Sie auf den Button „Weitere Einstellungen …“

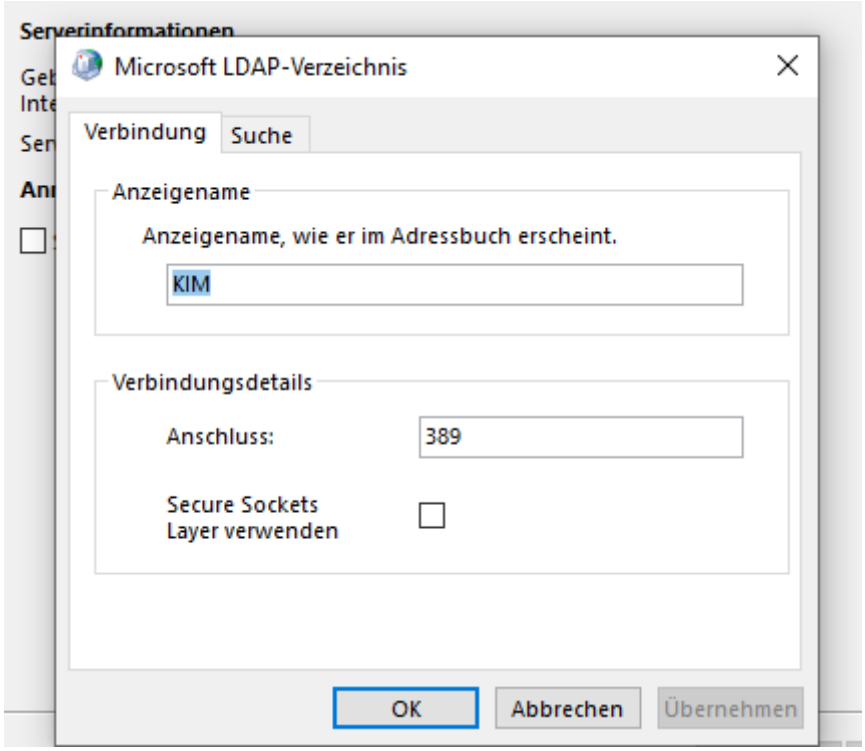

Abbildung 88: Outlook – Konfiguration der LDAP-Verbindung

Tragen Sie den Adressbuchnamen ein, so wie er später angezeigt werden soll, und ergänzen Sie dann die Verbindungsdetails.

Hinweis:
Achten Sie darauf, dass der Port für LDAP auf 389 und LDAPs auf 636 lautet. Bei Verwendung des Port 636 muss „Secure Sockets Layer verwenden“ angehakt werden.

- Wechseln Sie den Tab auf „Suche“:

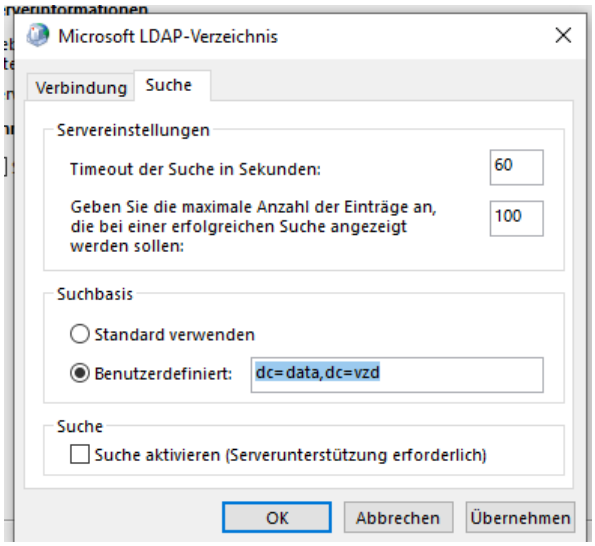

Abbildung 89: Outlook – Konfiguration der LDAP-Suche

Geben Sie nun die Suchbasis, wie in Abbildung 89 dargestellt ein.

- Schließen Sie die Konfiguration und Übernahme der Daten mit „OK“ ab.

Das zentrale KIM-Verzeichnis sollte Ihnen nun in etwa wie folgt angezeigt werden:

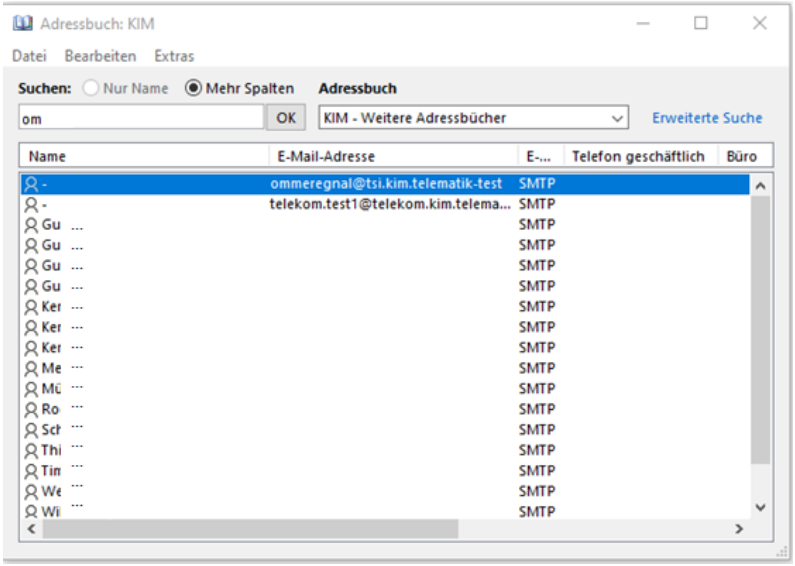

Abbildung 90: Beispiel-Adressbuch PU

Damit ist die Konfiguration des zentralen Adressbuchs in Outlook abgeschlossen.

A Anhang

A.1 Literaturverzeichnis

[gemSpec_CM] KIM-Clientmodulspezifikation, Version 1.16.0 vom 24.04.2023, gematik

A.2 BSI-Regelung ORP.4.A8: Regelung des Passwortgebrauchs

Die Institution MUSS den Passwortgebrauch verbindlich regeln (siehe auch ORP.4.A22 Regelung zur Passwortqualität und ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme). Dabei MUSS geprüft werden, ob Passwörter als alleiniges Authentisierungsverfahren eingesetzt werden sollen, oder ob andere Authentisierungsmerkmale bzw. -verfahren zusätzlich zu oder anstelle von Passwörtern verwendet werden können.

- Passwörter DÜRFEN NICHT mehrfach verwendet werden.
- Für jedes IT-System bzw. jede Anwendung MUSS ein eigenständiges Passwort verwendet werden.
- Passwörter, die leicht zu erraten sind oder in gängigen Passwortlisten geführt werden, DÜRFEN NICHT verwendet werden.
- Passwörter MÜSSEN geheim gehalten werden.
- Sie DÜRFEN NUR dem Benutzer persönlich bekannt sein.
- Passwörter DÜRFEN NUR unbeobachtet eingegeben werden.
- Passwörter DÜRFEN NICHT auf programmierbaren Funktionstasten von Tastaturen oder Mäusen gespeichert werden.
- Ein Passwort DARF NUR für eine Hinterlegung für einen Notfall schriftlich fixiert werden. Es MUSS dann sicher aufbewahrt werden.
- Die Nutzung eines Passwort-Managers SOLLTE geprüft werden. Bei Passwort-Managern mit Funktionen oder Plug-ins, mit denen Passwörter über Onlinedienste Dritter synchronisiert oder anderweitig an Dritte übertragen werden, MÜSSEN diese Funktionen und Plug-ins deaktiviert werden.
- Ein Passwort MUSS gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.

A.3 BSI-Regelung ORP.4.A22: Regelung zur Passwortqualität

In Abhängigkeit von Einsatzzweck und Schutzbedarf MÜSSEN sichere Passwörter geeigneter Qualität gewählt werden. Das Passwort MUSS so komplex sein, dass es nicht leicht zu erraten ist. Das Passwort DARF NICHT zu kompliziert sein, damit der Benutzer in der Lage ist, das Passwort mit vertretbarem Aufwand regelmäßig zu verwenden.

A.4 Liste verwendeter Cipher-Suiten

Folgende Cipher-Suiten kommen zum Einsatz:

Name der Cipher-Suite
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Tabelle 39: Verwendete Cipher-Suiten

A.5 Liste verwendeter Ports

Hinweis: Die verwendeten Ports hängen von den konfigurierten Parametern (z.B. mit oder ohne TLS) ab. Dies ist zu berücksichtigen.

Folgende Ports sollten für TCP bzw. UDP freigeschaltet sein:

Port	Verwendung
25	SMTP
53	DNS
110	POP3
389	LDAP
443	Konnektor via TLS
465	SMTPs
636	LDAPs
995	POP3s
996	POP3s[8]

Tabelle 40: Verwendete Ports

[8] Bei Verwendung des Clientmoduls zusammen mit dem KIM-Security-Interface

A.6 Abkürzungsverzeichnis

Abkürzung	Bedeutung
AMSI	Antimalware Scan Interface
BPjM	Bundesprüfstelle für jugendgefährdende Medien
CM	Clientmodul
DNS	Domain Name Service
DNS-SD	Domain Name Service – Service Discovery
DTHS	Deutsche Telekom Health Services
DVO	Dienstleister vor Ort
Ggü	Gegenüber
Abkürzung	Bedeutung
AMSI	Antimalware Scan Interface
BPjM	Bundesprüfstelle für jugendgefährdende Medien
CM	Clientmodul
DTHS	Deutsche Telekom Health Services
DVO	Dienstleister vor Ort
Ggü	Gegenüber
GmbH	Gesellschaft mit beschränkter Haftung
GUI	Graphical User Interface
HBA	Heilberufeausweis
ICCSN	Integrated Circuit Card Serial Number
ID	Identity
IP	Internet Protocol
JDK	Java Development Kit
JKS	Java Key Store
KIM	Kommunikation im Gesundheitswesen
KOM-LE	Kommunikation der Leistungserbringer
LDAP	Lightweight Directory Access Protocol
OS	Operating System
PIN	Personal Identity Number
PIN	Personal Identity Number
PKCS12	Public-Key Cryptography Standard N. 12

PKI	Public Key Infrastructure
POP3	Post Office Protocol Version 3
PU	Produktionsumgebung
RU	Realisierungsumgebung
SMC-B	Secure Module Card, Bauart B
SMTP	Simple Mail Transport Protocol
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
SW	Software
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TU	Testumgebung
URI	Uniform Resource Identifier
usw	Und so weiter
VZD	Verzeichnisdienst

Tabelle 41: Abkürzungsverzeichnis